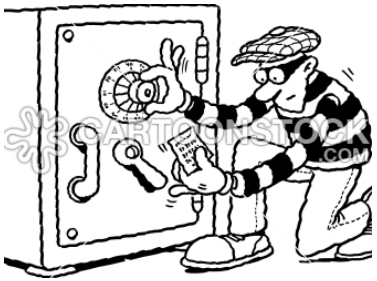
Design Automation for Cryptography

Anupam Chattopadhyay
Assistant Professor, School of Computer Science and Engineering
School of Physical and Mathematical Sciences, Nanyang Technological University
June 7, 2017

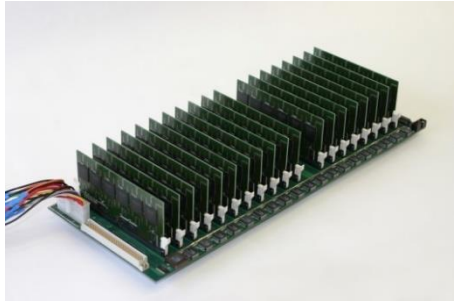
NANYANG TECHNOLOGICAL UNIVERSITY

Motivation

- Security *not* a feature but a design metric
- Crytography is highly dynamic



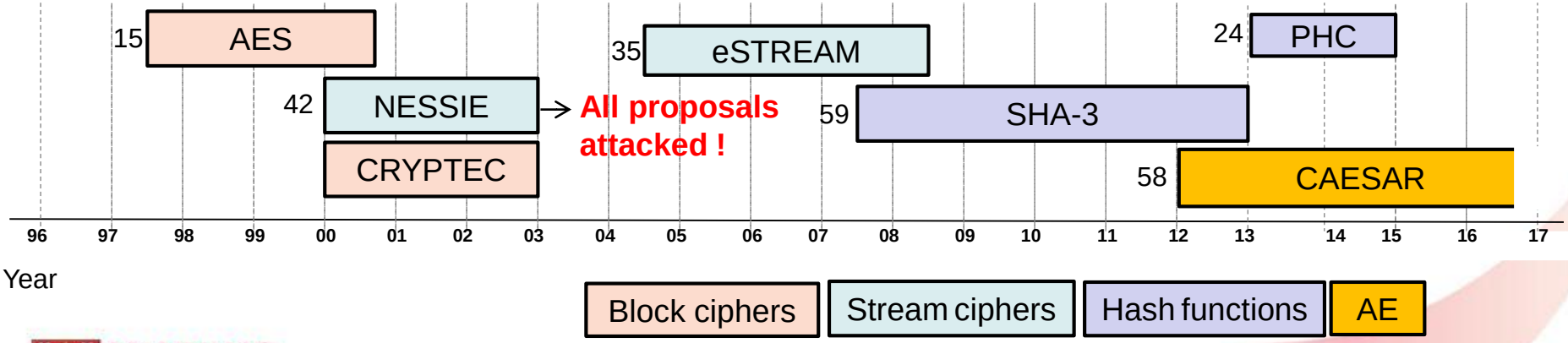
Cryptanalysis



Custom cryptanalysis]

Lightweight cryptography

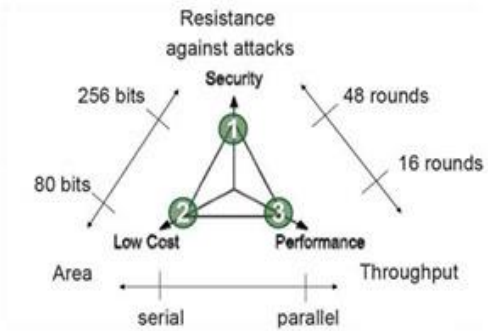
- **Timeline of cryptgraphic competitions**



NANYANG TECHNOLOGICAL UNIVERSITY

Motivation

- Design metrics



- Security kerenels developer has a huge design space

Variety of constraints
Area footprint, power utilization, latency, operating frequency, cost, ...

Variety of target platforms
GPPs, DSP, GPUs, ASICs, ASIPs, FPGAs, CPLDs, Microcontrollers, ...

Variety of requirements
Throughput, security, thermal limitations, distribution, scalability, flexibility, ...

Architectural customization
Wordsize, instruction set, Memory, microarchitectural template, Interfaces, ...

Contents

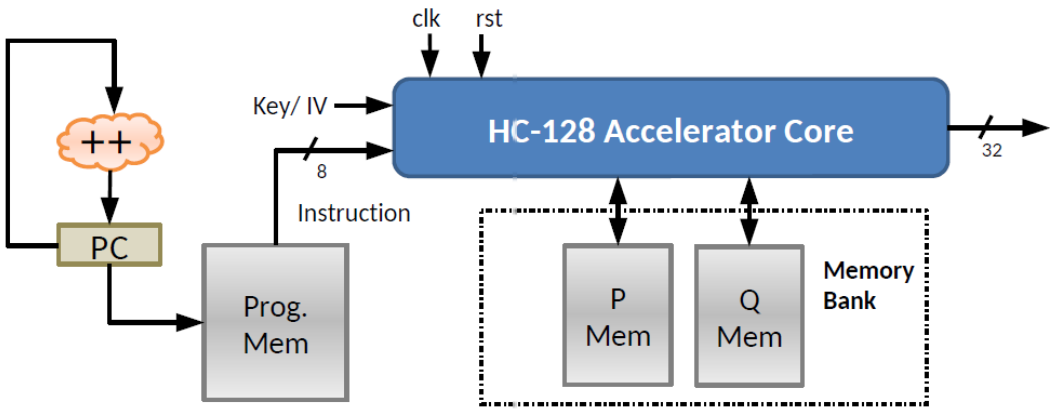
Custom Optimization Examples

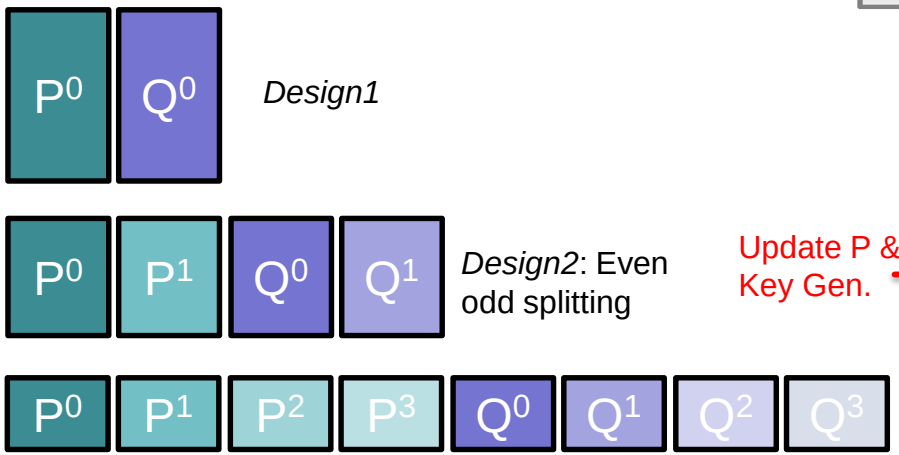
- Domain-specific High Level Synthesis
- Fault-resistant Design by Physical Synthesis

NANYANG TECHNOLOGICAL UNIVERSITY

HC-128: Parallelization by State Splitting

- P and Q has 512 words of 32-bit
- 5 reads, 1 write





Update P & Key Gen.

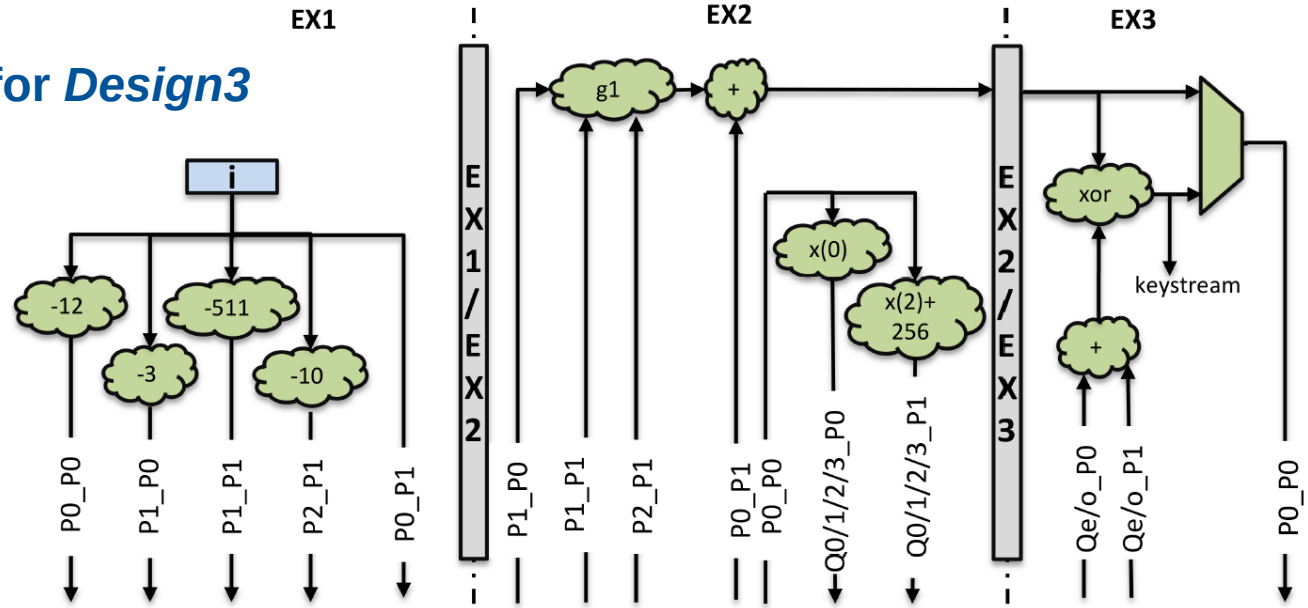
$$
\begin{aligned}
&\text{if } (i \bmod 1024) < 512 \\
&\{ \\
&\quad P[j] = P[j] + g_1(P[j \boxminus 3], P[j \boxminus 10], P[j \boxminus 511]); \\
&\quad s_i = h_1(P[j \boxminus 12]) \oplus P[j]; \\
&\} \\
&\text{else} \\
&\{ \\
&\quad Q[j] = Q[j] + g_2(Q[j \boxminus 3], Q[j \boxminus 10], Q[j \boxminus 511]); \\
&\quad s_i = h_2(Q[j \boxminus 12]) \oplus Q[j]; \\
&\}
\end{aligned}
$$

NANYANG TECHNOLOGICAL UNIVERSITY

A. Khalid, et al. One Word/Cycle HC-128 Accelerator via State-Splitting Optimization, in INDOCRYPT 2014

HC-128: Parallelization by State Splitting

Pipeline for *Design3*



Design	Clock Freq. (GHz)	Core area (KGE)			Memory			Total Area (KGE)
		Comb.	Sequential	Total	Organization	(Bytes)	(KGE)	
*Design*1	1.20	5.47	1.64	5.55	2x512	4096	53.22	58.77
*Design*2	1.30	9.63	1.38	8.60	4x256	4096	72.56	81.16
*Design*3	1.35	16.24	1.17	13.61	8x128	4096	110.4	124.01

Design	Clock Freq. (GHz)	Initialization latency		Throughput		TPA (Gbps/KGE) with	
		(cycles)	(ms)	(cycles/word)	(Gbps)	Core Area	Total Area
*Design*1	1.20	9168	7.64	4	9.60	1.73	0.16
*Design*2	1.30	4584	3.53	2	20.80	2.42	0.26
*Design*3	1.35	3556	2.63	1	43.20	3.18	0.35

NANYANG TECHNOLOGICAL UNIVERSITY

Faraday 65m Standard Cell library, typical case

AES: Technology Mapping

- The AES MixColumns: matrix multiplication operation of the AES state byte matrix by a constant matrix given by

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

- The smallest circuit in literature requires **108 XOR gates** to implement this.
  - This function is four instances of the following equation over :

  → **41 LUTs** using the LUT6 FPGA technology.

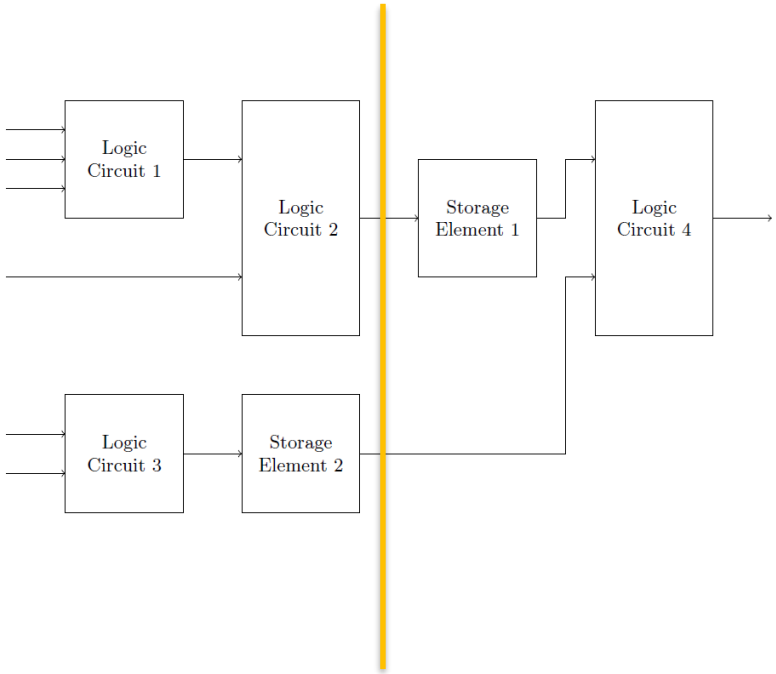
$$p = 2 \cdot a \oplus 3 \cdot b \oplus c \oplus d$$

- Instead, we view the operation as a Boolean function rather than over and we optimize it towards an implementation of **36 LUTs**.
- Inverse MixColumns similarly can be reduced from **72** to **60 LUTs**.

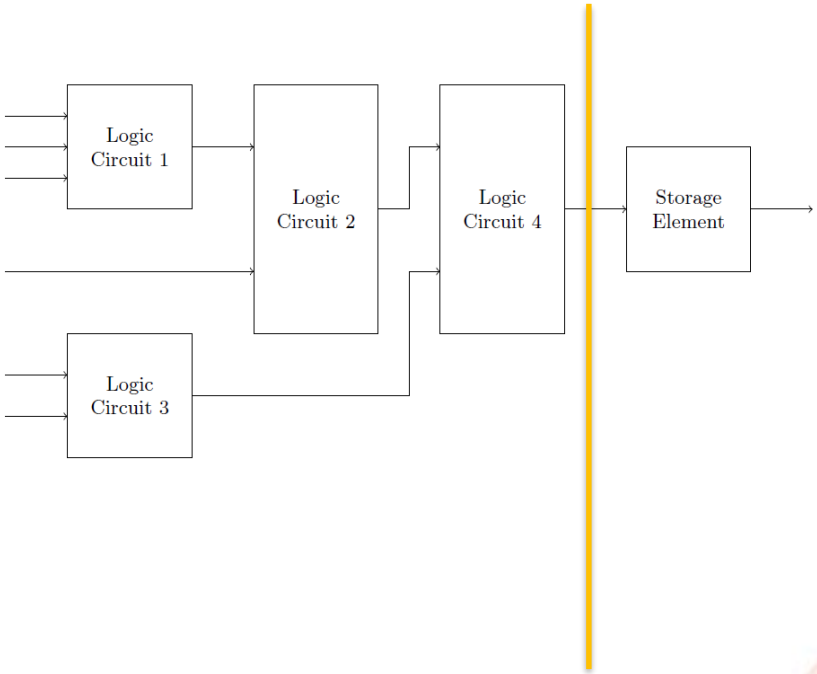
NANYANG TECHNOLOGICAL UNIVERSITY

Joint work with Mustafa Khairallah and Thomas Peyrin, unpublished

FPGA-Aware Pipelining



Logic-aware Partitioning



FPGA-aware Partitioning

NANYANG TECHNOLOGICAL UNIVERSITY

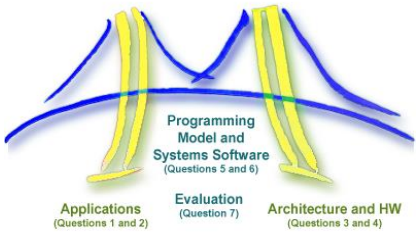
Joint work with Mustafa Khairallah and Thomas Peyrin, unpublished

High-Level Synthesis

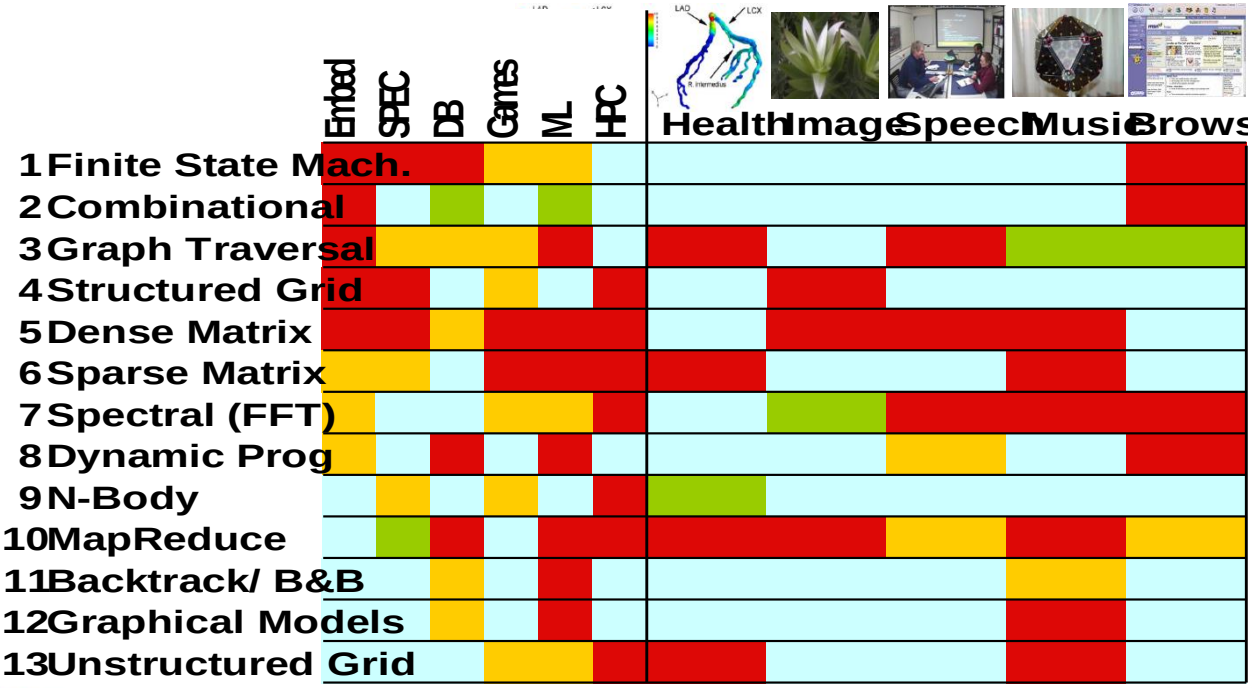
- Focuses on algorithm to RTL flow
  - × Dependent on user proficiency, varies widely from tool to tool
  - × Unaware of technology platforms
  - × Hard to reuse design knowledge
  - × Storage allocation optimizations missing

Domain-specialization?

Berkeley Dwarfs for Parallel Computing[1]



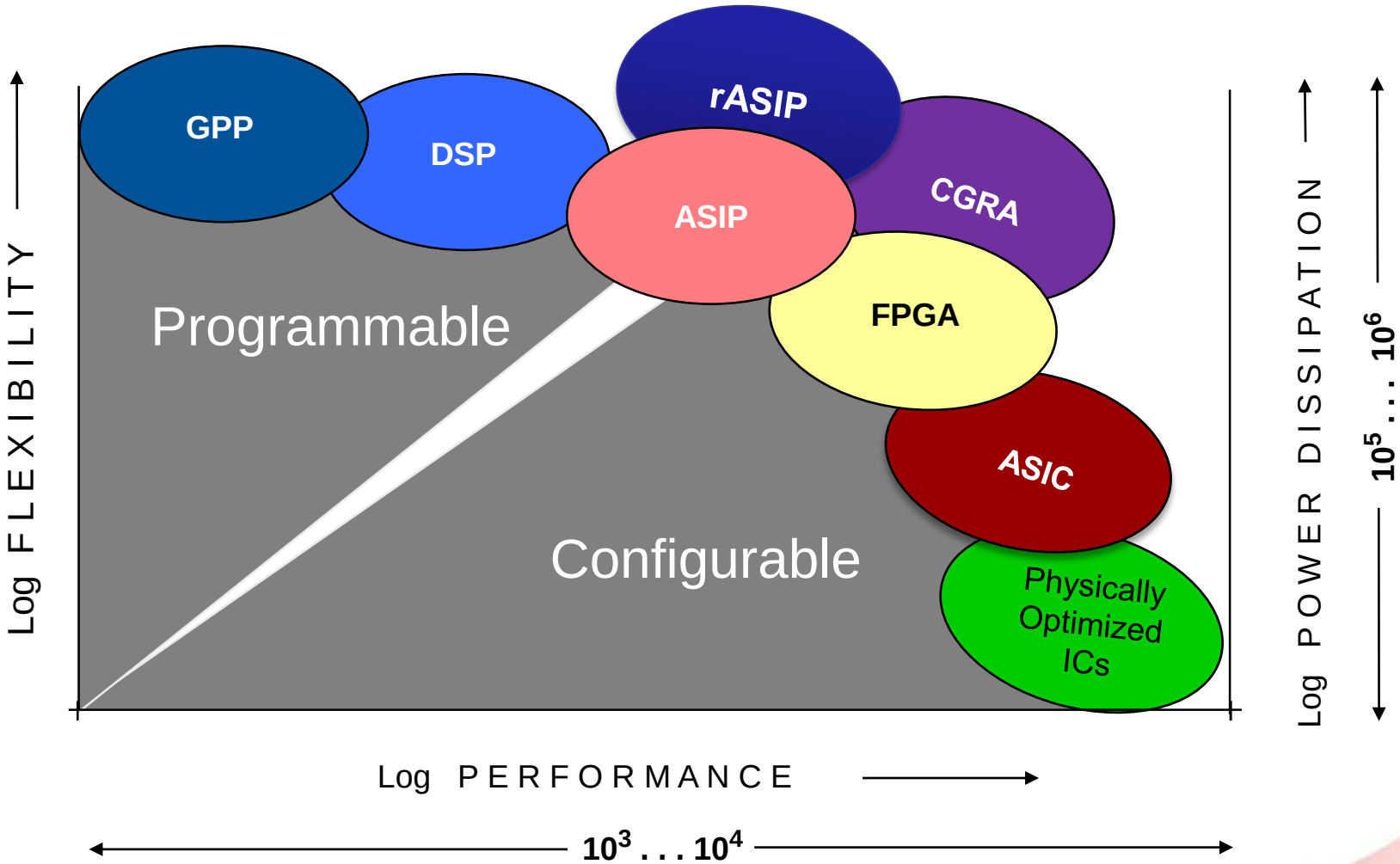
- How apps relate to 13 dwarfs (Red Hot → Blue Cool)



NANYANG TECHNOLOGICAL UNIVERSITY

[1] The Landscape of Parallel Computing Research: A View from Berkeley, by K. Asanovic et al , Technical Report, 2006

SoC Processing Elements



Source: T. Noll, RWTH Aachen

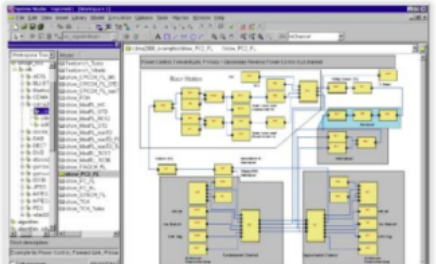
Domain-specific High Level Synthesis: Lessons from Wireless Communication IP

System Studio

Overview

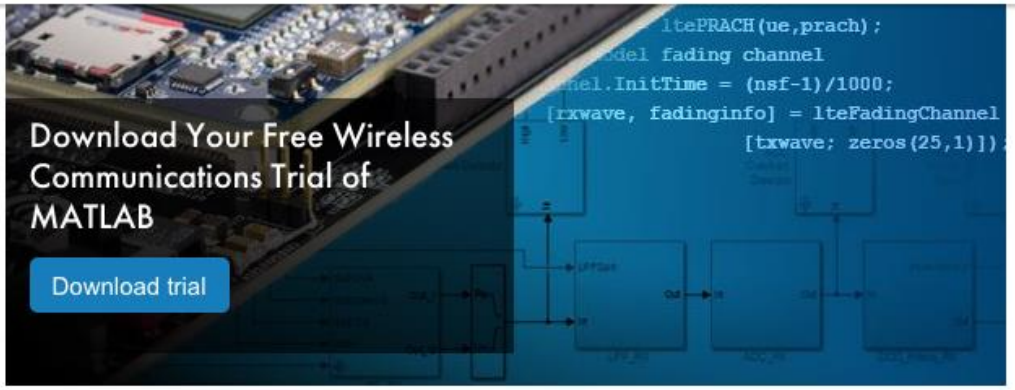
System Studio is a high performance, model-based signal processing algori
combines the industry's best simulation performance with high modeling ef
chip implementation design and verification flows. Leading communication
Synopsys' System Studio and DSP model libraries to address their system-l
faster. There is a good chance that your cell phone comes with a System St

Download Datasheet



Wireless Communications Design with MATLAB

Search



Wireless engineering teams use today's MATLAB® to reduce development time, from algorithm development through full system simulation and hardware implementation. These engineers save time and eliminate steps by:

- **Proving algorithm concepts** in simulation and over-the-air tests
- **Exploring and optimizing system behavior** with models that include digital, RF, antenna elements
- **Eliminating design problems** before moving to implementation

NANYANG TECHNOLOGICAL UNIVERSITY

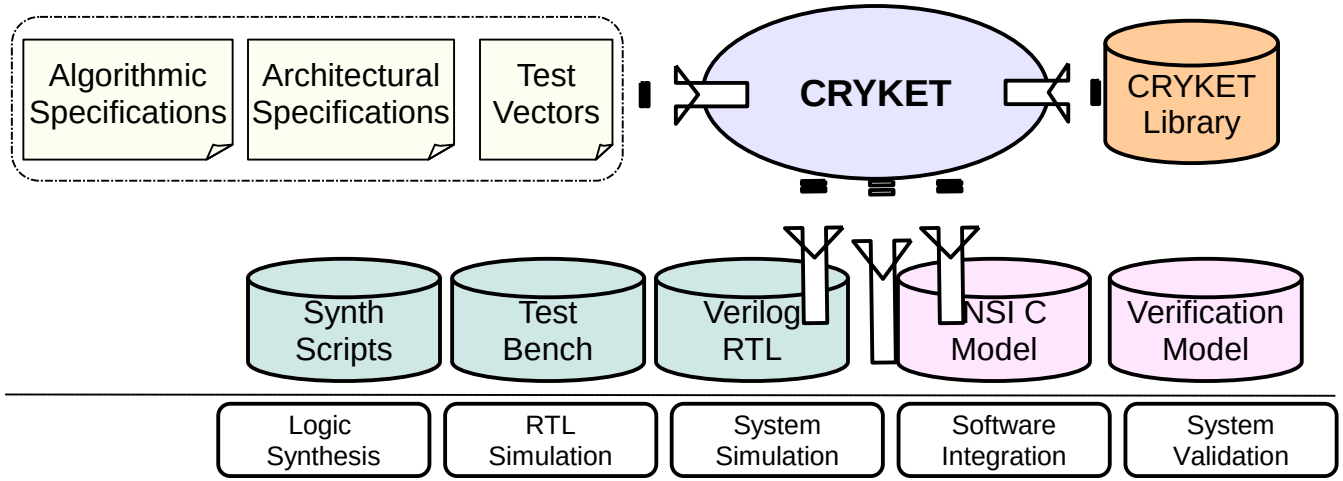
Contents

- Custom Optimization Examples
- *Domain-specific High Level Synthesis*
- Fault-resistant Design by Physical Synthesis

NANYANG TECHNOLOGICAL UNIVERSITY

CRYKET: Overview

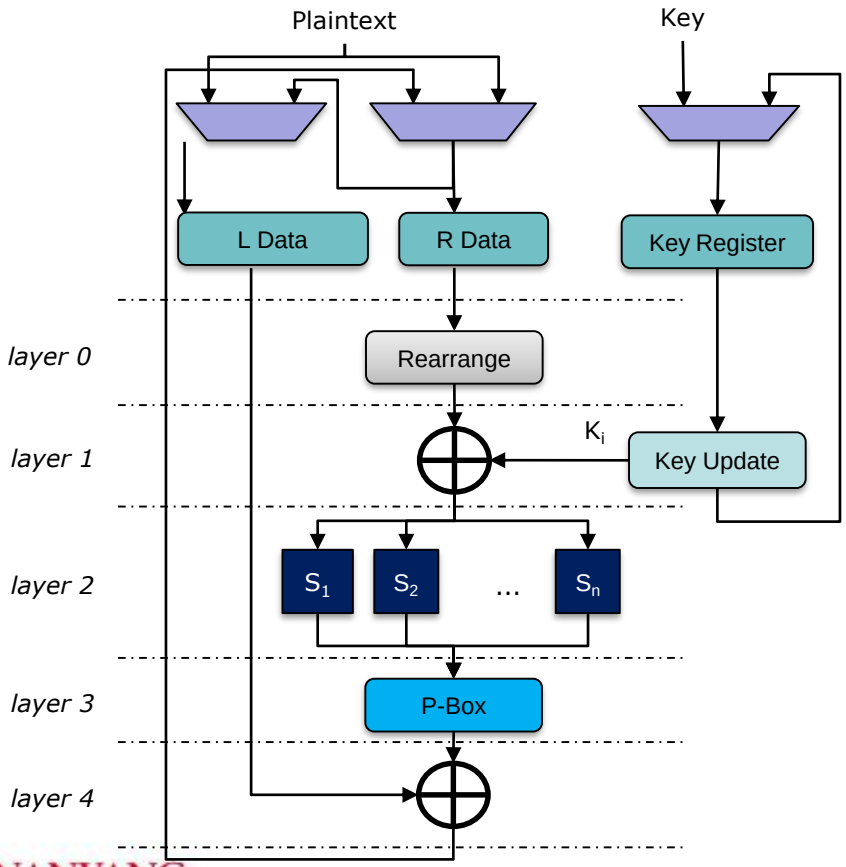
- CRYKET (Cryptographic Kernels Toolkit): Domain specific HLS
  - *Language independent* GUI based design capture
  - Domain specific expertise, well understood kernels



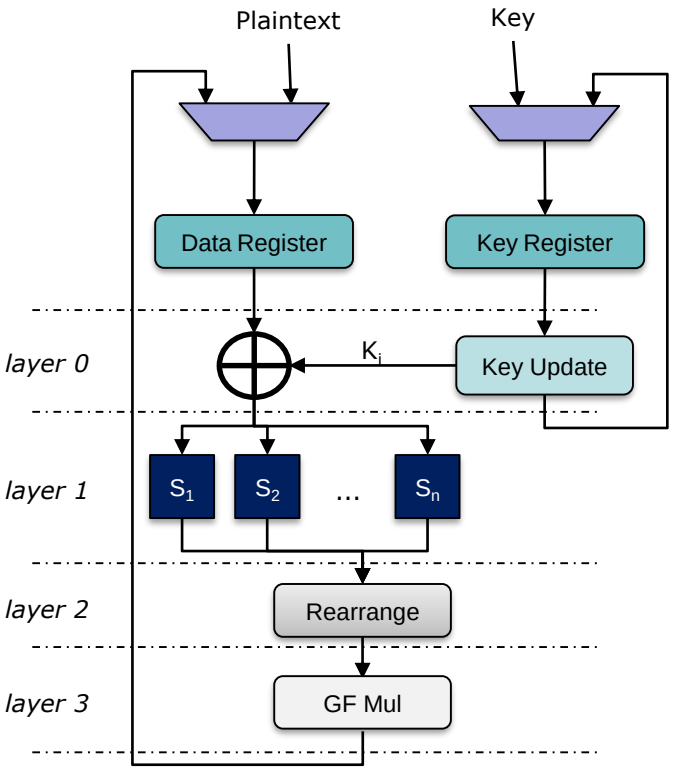
A. Khalid, et al. RAPID-FeinSPN: A Rapid Prototyping Framework for Feistel and SPN-Based Block Ciphers. ICISS 2013

RunFein: Feistel and SPN Block Cipher

- Block/key/word sizes, rounds, mode of operation, test vectors
- Layers of operation: S/P-Box, Bitwise/ Arithmetic/Boolean/ Field operations, compound popular cipher operations



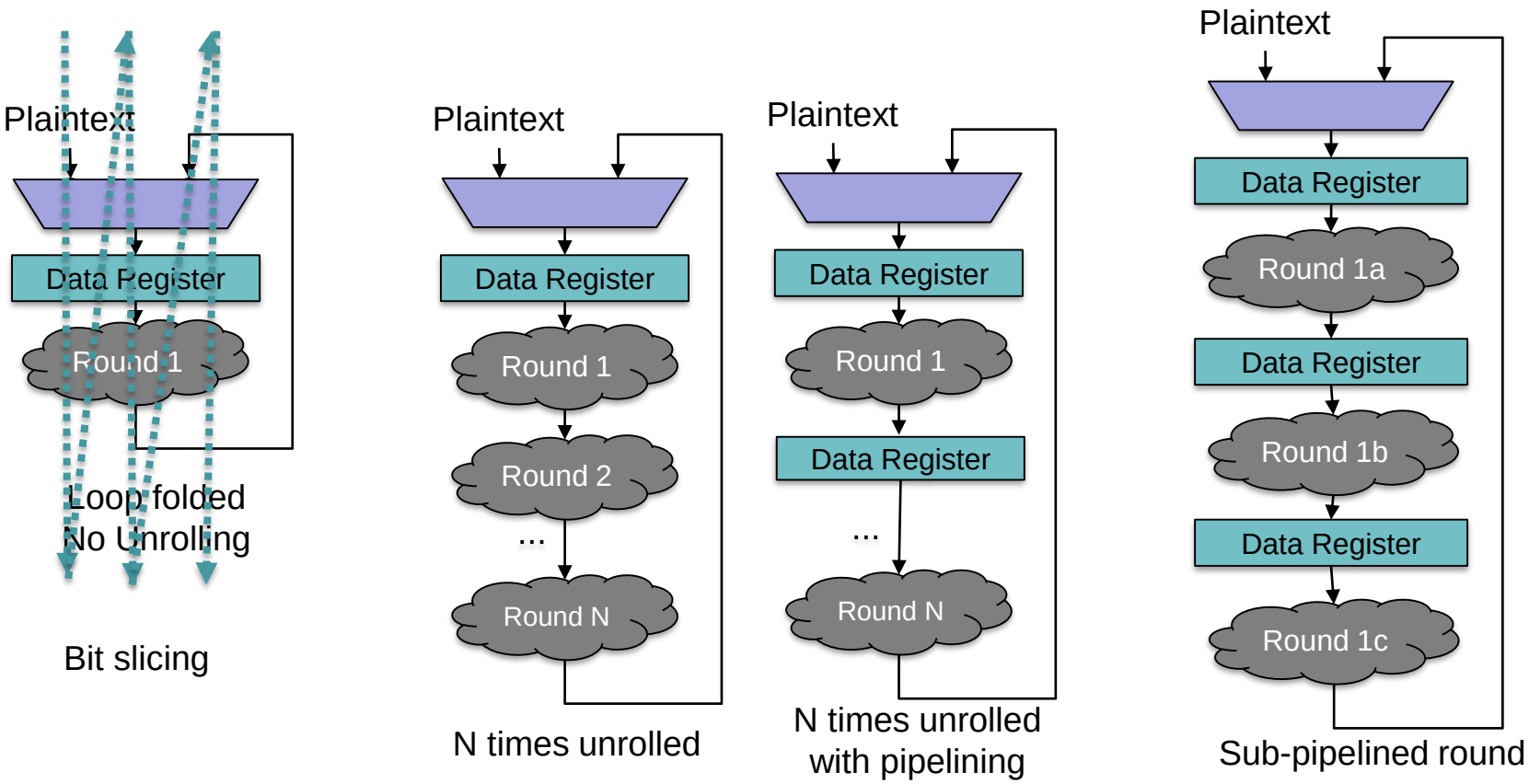
Feistel Network cipher



SPN Cipher

A. Khalid, et al. RunFein: A Rapid Prototyping Framework for Feistel and SPN Based Block Ciphers, JCEN 2016

RunFein: Fast Design Space Exploration



A. Khalid, et al. RunFein: A Rapid Prototyping Framework for Feistel and SPN Based Block Ciphers, JCEN 2016

RunFein: GUI

Defines | Key Scheduler | SBOX Values | PBOX Values | NIST Test Suite

Basic Parameters

Block Size 128 Multiple of 2
Word Size 8 Less than Block Size
Round Start 1
Round End 10
Key Size 128 >= Block Size

Microarchitecture

Unroll Factor 1 Less than Round End
Pipeline ☐ Between rounds
Subpipeline ☐ Between ops
Bit slicing ☐ 4 Word Length

Cipher Modes
Mode ECB Encryption
IV 00000000000000000000000000000000

Operations

Initialization
# of operations 1 ← round_init
Operation 1 AddRoundKey
SBOX
PBOX
Rotate
GaloisFieldMul
ShiftRows
Custom

Rounds
# of operations 4 ← round_middle
Operation 1 SBOX
Operation 2 ShiftRows
Operation 3 GaloisFieldMul
Operation 4 AddRoundKey

Finalization
# of operations 3 ← round_final
Operation 1 SBOX
Operation 2 ShiftRows
Operation 3 AddRoundKey

Edit
Save
AES-128

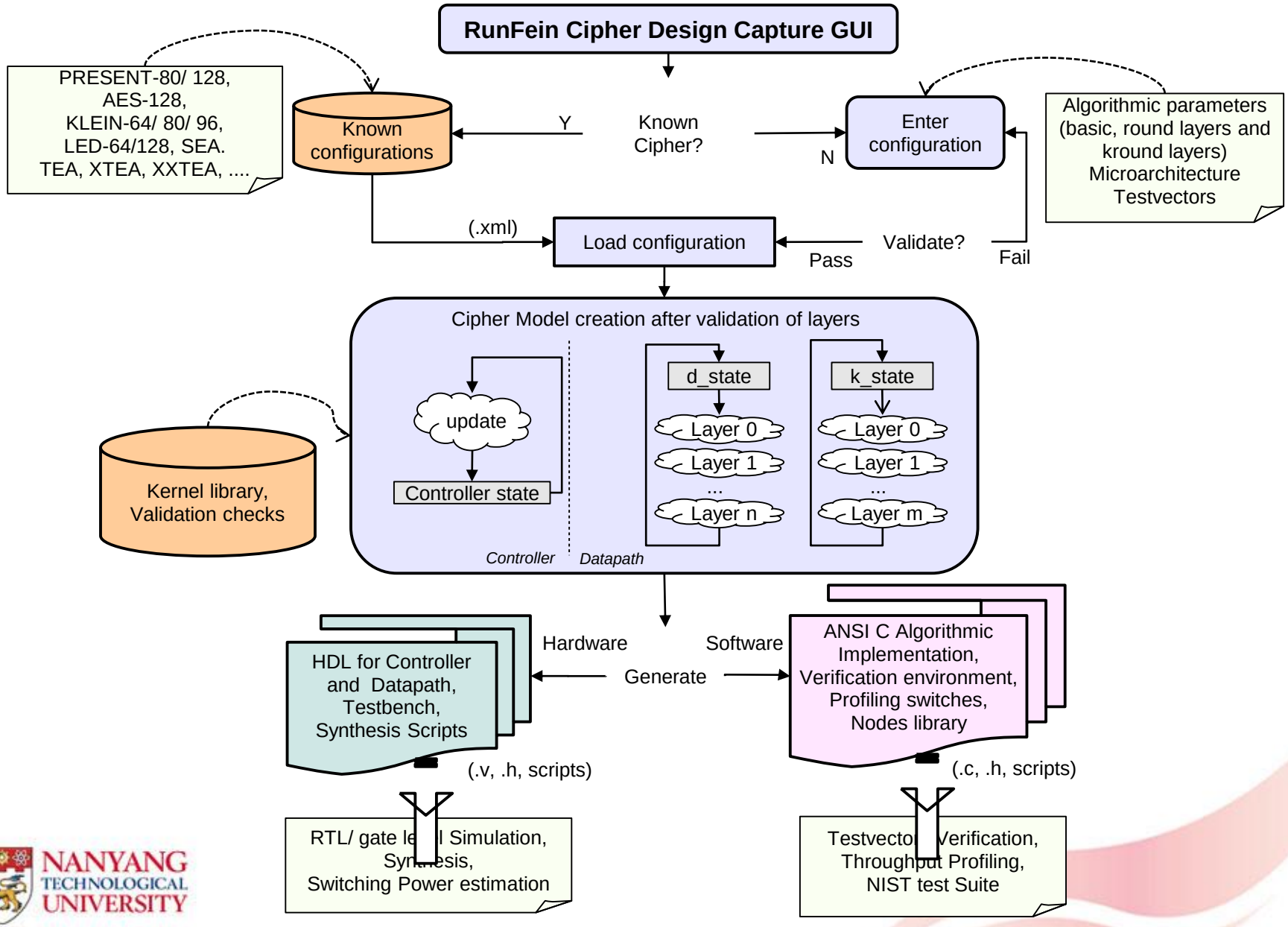
CRYKET

Load Key File path
Cipher Key 00000000000000000000000000000000
Load Plain Text File path
Plain Text

Generate C Code | Generate LISA Code | Exit

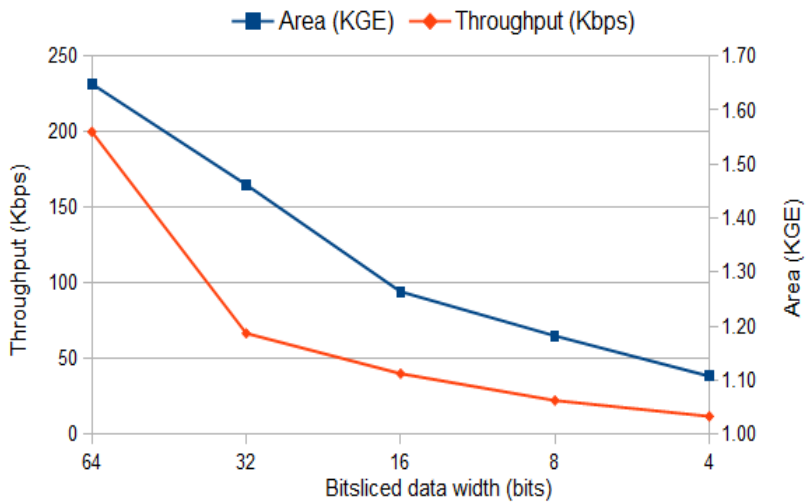
Log date/time : Thu Mar 6 09:19:23 2014

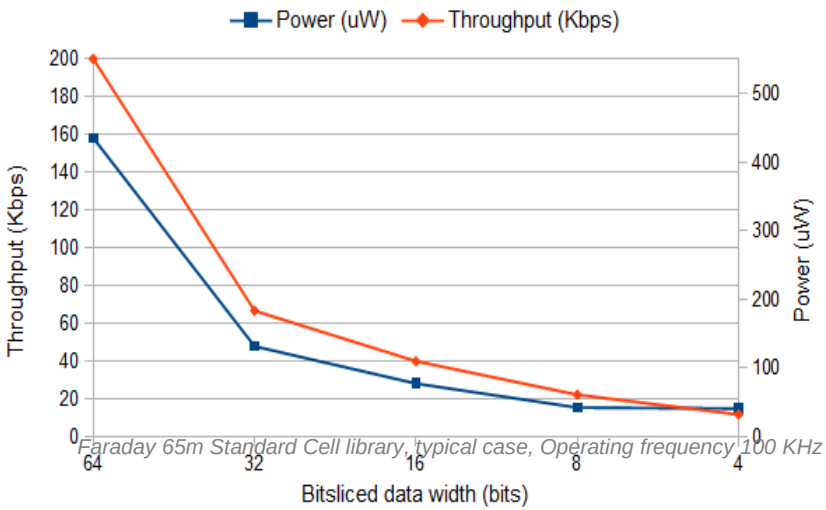
NANYANG TECHNOLOGICAL UNIVERSITY



NANYANG TECHNOLOGICAL UNIVERSITY

RunFein: PRESENT-80 Bitslicing





Faraday 65m Standard Cell library, typical case, Operating frequency 100 KHz

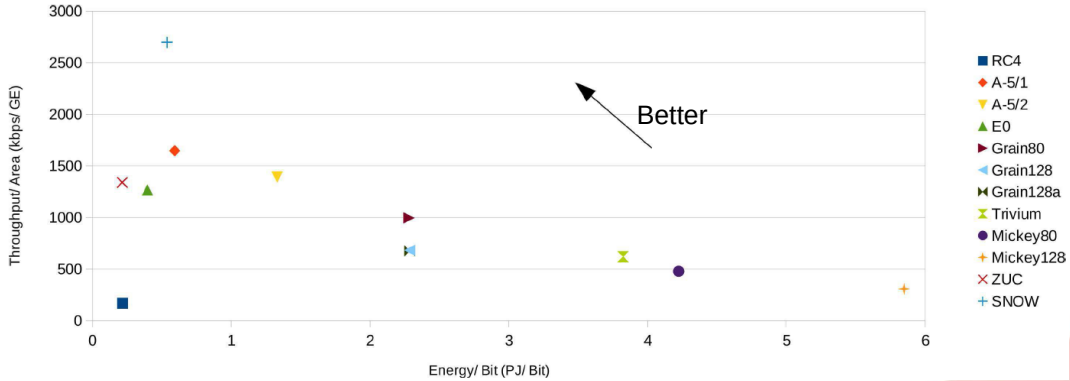
	Area (GE) RunFein			Area (GE) [1]		
(S_b)	65nm	90nm	180nm	180nm	250nm	350nm
64	1649	1519	1751	1650	1594	1525
32	1462	1379	1602	-	-	-
16	1264	1203	1403	-	-	-
8	1182	1121	1313			-
4	1107	1081	1265	1075	1169	1000

NANYANG TECHNOLOGICAL UNIVERSITY

Faraday 65m Standard Cell library, typical case, Synopsys Design Compiler F-2011.09

RunStream: Analysis and Results

	Classification/Construction											Salient Features					
	Synchronous	Additive	Binary	LFSR	CLFSR	NFSR	Jump Registers	FSM Registers	Irregular Clocking	Multiple Generators	Nonlinear Filter	Granularity (bits)	Key (bits)	IV (bits)	key setup (cycles)	Randomization (cycles)	Initialization (cycles)
A-5/1	✔	✔	✔	✔	✗	✗	✗	✗	✔	✔	✗	1	64	22	86	100	186
A-5/2	✔	✔	✔	✔	✗	✗	✗	✗	✔	✔	✔	1	64	22	86	100	186
E0	✔	✔	✔	✔	✗	✗	✗	✔	✗	✔	✔	1	8-128	-	200	128	328
Grain80	✔	✔	✔	✔	✗	✔	✗	✗	✗	✔	✔	1	80	64	160	160	320
Grain128	✔	✔	✔	✔	✗	✔	✗	✗	✗	✔	✔	1	128	96	256	256	512
Grain128a	✔	✔	✔	✔	✗	✔	✗	✗	✗	✔	✔	1	128	96	256	256	512
Trivium	✔	✔	✔	✔	✗	✗	✗	✗	✗	✔	✗	1	80	80	288	1152	1440
MICKEY80-v2	✔	✔	✔	✗	✗	✔	✔	✗	✔	✔	✗	1	80	80	160	100	260
MICKEY128	✔	✔	✔	✗	✗	✔	✔	✗	✔	✔	✗	1	128	128	256	160	416
RC4	✔	✔	✗	✗	✗	✗	✗	✔	✗	✗	✔	8	40-2K	-	256	256	512
ZUC	✔	✔	✗	✗	✗	✔	✗	✔	✗	✗	✔	32	128	128	16	32	48
SNOW 3G	✔	✔	✗	✗	✗	✔	✗	✔	✗	✗	✔	32	128	128	16	32	48



NANYANG TECHNOLOGICAL UNIVERSITY

A. Khalid, et al. RunStream: A High-level Rapid Prototyping Framework for Stream Ciphers. In ACM TECS, 2016

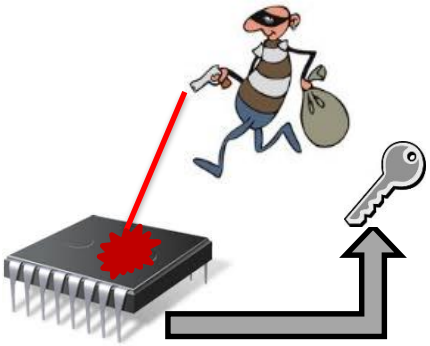
Contents

- Custom Optimization Examples
- Domain-specific High Level Synthesis
- *Fault-resistant Design by Physical Synthesis*

NANYANG TECHNOLOGICAL UNIVERSITY

Preventing Differential Fault Analysis Attack

- Attacker assumptions
  - Ability to induce fault at a given time (T) and space (S) precision
  - Ability to infer/solve a system of equations based on the observed faulty (CT^*) and correct (CT) ciphertext



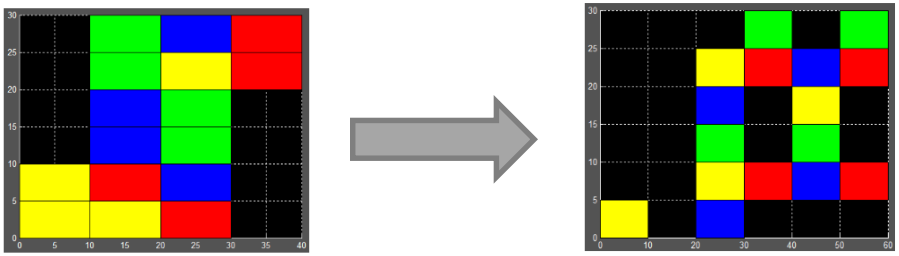
- Prevention
  - Redundancy, Concurrent Error Detection
  - Attack-specific mounted sensor

DFARPA: Differential Fault Attack Resistant Physical Design Automation

- Exemplary Fault Attack on AES[1]
  - Multi-byte fault attack model
  - Fault is induced in at least one of the four diagonals in the AES state

D0	D1	D2	D3
D3	D0	D1	D2
D2	D3	D0	D1
D1	D2	D3	D0

- Solution: Generate floorplan for the 16 blocks, so that the fault become un-exploitable in presence of the fault cluster of radius r units
  - Place the blocks(elements) of each diagonal at least r units distance
  - Formulated as a constrained placement problem



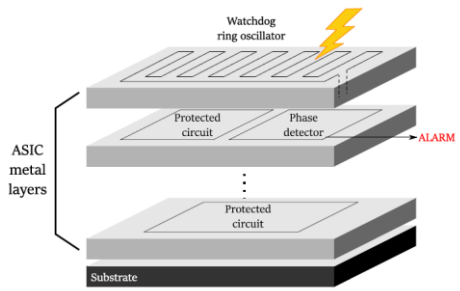
1. D. Saha, D. Mukhopadhyay, and D. RoyChowdhury. A diagonal fault attack on the advanced encryption standard. Cryptology ePrint Archive, Report 2009/581, 2009. http://eprint.iacr.org/2009/581.

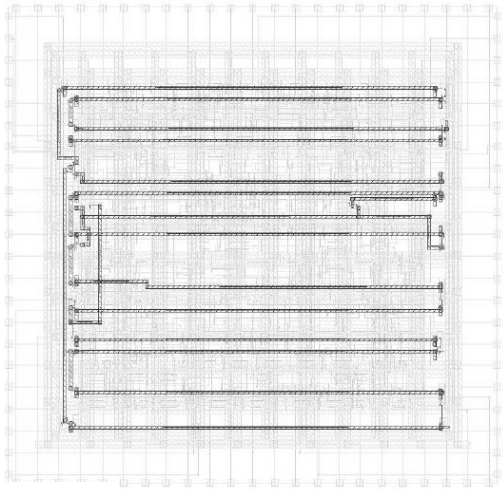
Joint work with Debdeep Mukhopadhyay and Shivam Bhasin, unpublished

NANYANG TECHNOLOGICAL UNIVERSITY

DFARPA: Reactive Countermeasure

- The sensor is composed of two key components
  - a watchdog ring oscillator (WRO) and a phase detection (PD) circuit.
- High energy injections impact signal propagation delay, which disturbs the phase of WRO. This phase change is detected by the PD circuit to raise an alarm and halt sensitive computation.





- 2 Metal layers are reserved for WRO routing

Table 4: Post-layout Results: Plantlet

Feature	Unprotected	Protected
Area (μm^2)	1293	1358 (5%)
Max. Path Delay (ns)	0.61	0.62 (1%)
Avg. Dynamic Power (μW)	259.26	551.5 (212%)
Utilization Factor	0.6	0.6 (0%)

NANYANG TECHNOLOGICAL UNIVERSITY

Joint work with Debdeep Mukhopadhyay and Shivam Bhasin, unpublished

Contents

- Custom Optimization Examples
- Domain-specific High Level Synthesis
- Fault-resistant Design by Physical Synthesis

NANYANG TECHNOLOGICAL UNIVERSITY

Conclusion and Outlook

- Conclusion
  - Domain-specific HLS can push the design efficiency and productivity
  - Different phases of EDA can integrate cryptographic/cryptanalyst knowhow to improve

- Outlook
  - Integrating (more) custom optimizations
  - Diverse technology/platform-specific constraints
  - Diverse cipher families
  - Integrating automated SCA and DFA protection

NANYANG TECHNOLOGICAL UNIVERSITY

Thank you!

Questions?

NANYANG TECHNOLOGICAL UNIVERSITY