KU LEUVEN

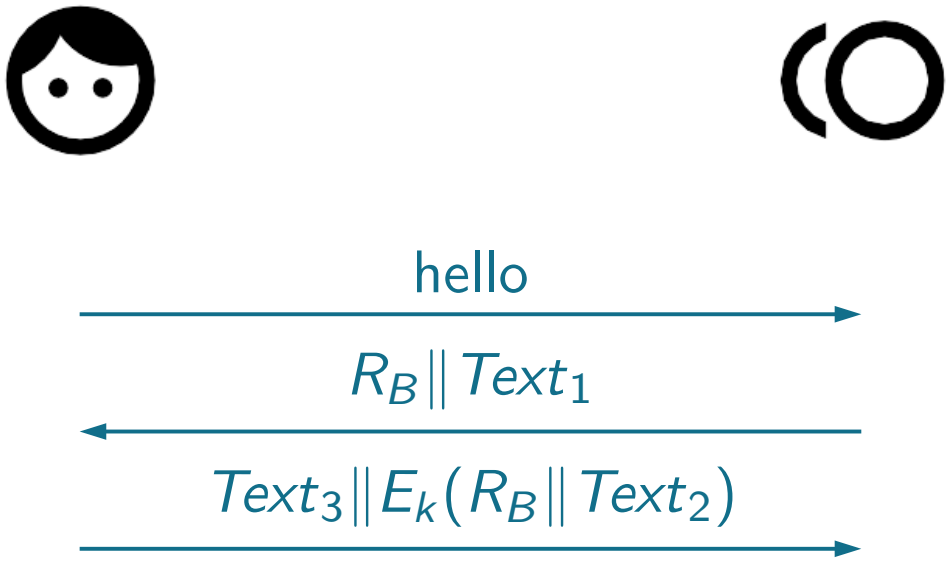
Single-Cycle Implementations of Block Ciphers

Pieter Maene and Ingrid Verbauwhede
KU Leuven/COSIC, Belgium

July 21, 2015

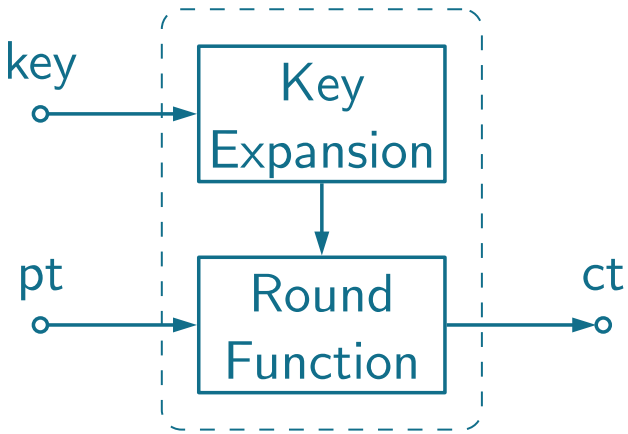
Outline

Introduction



Use-Case: Industrial Valve Control

- Fixed clock frequency in hostile environment
- Instantaneous reaction requires fast single-cycle encryption



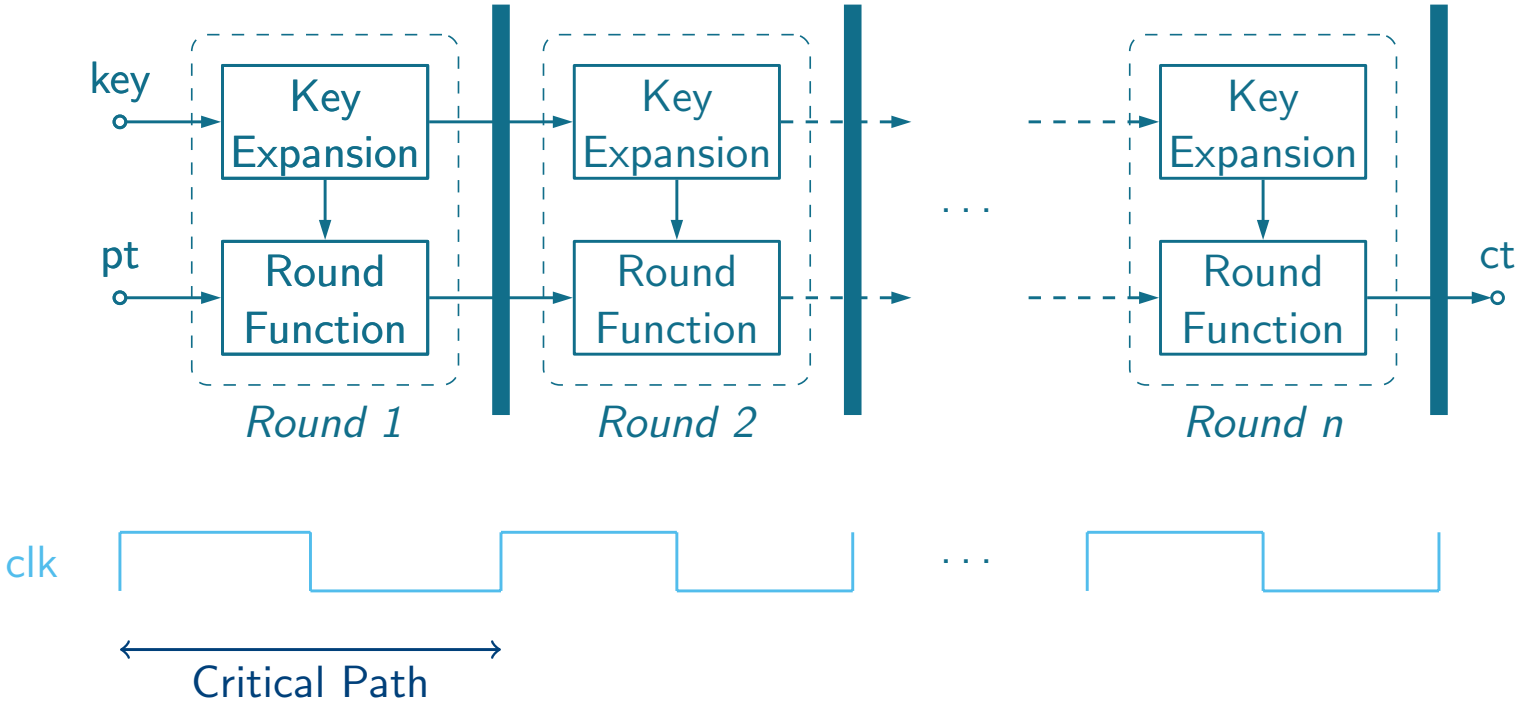
Latency
The delay from input to output

Throughput
Rate of encryption

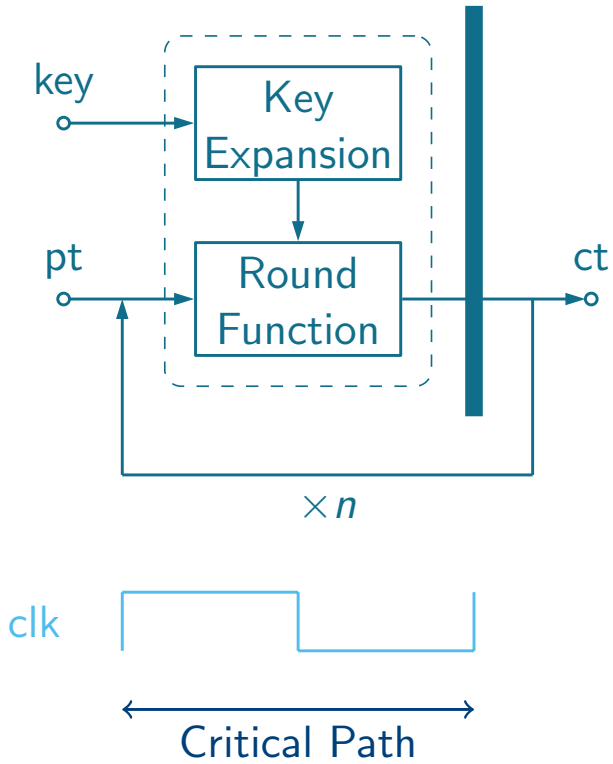
Critical Path
The slowest path between two registers

Three ways of implementing block ciphers in hardware.

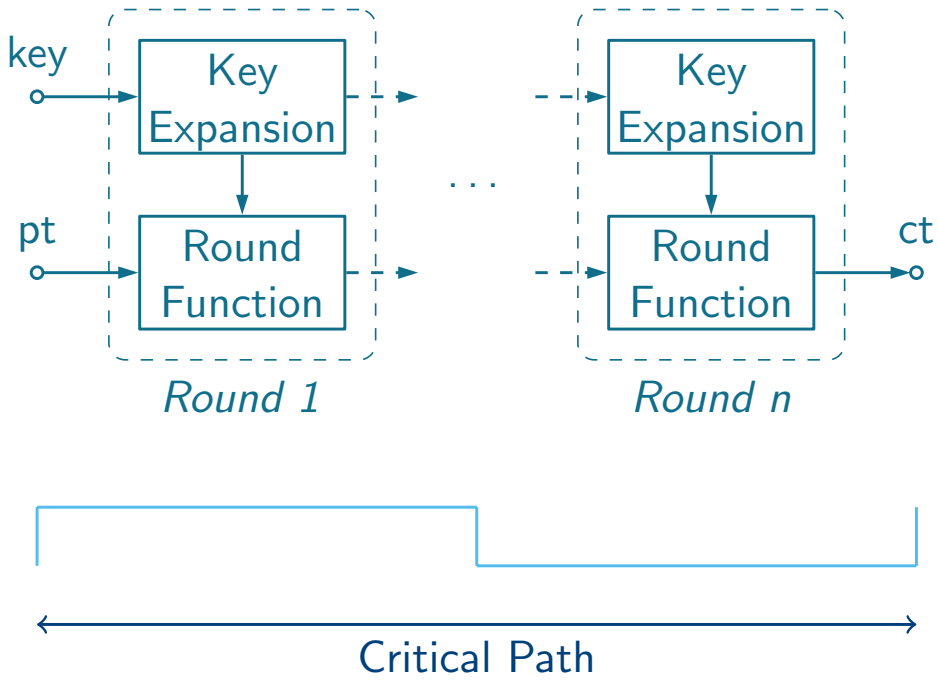
Pipelined



Latency: n ns **Throughput:** 1 Gbit/s **Critical Path:** 1 GHz



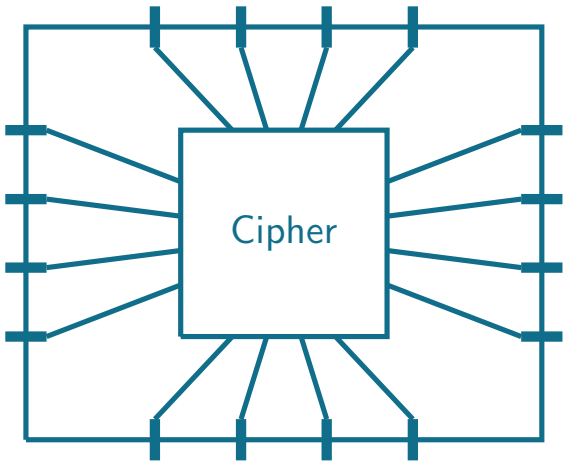
Latency: n ns **Throughput:** $\frac{1}{n}$ Gbit/s **Critical Path:** 1 GHz



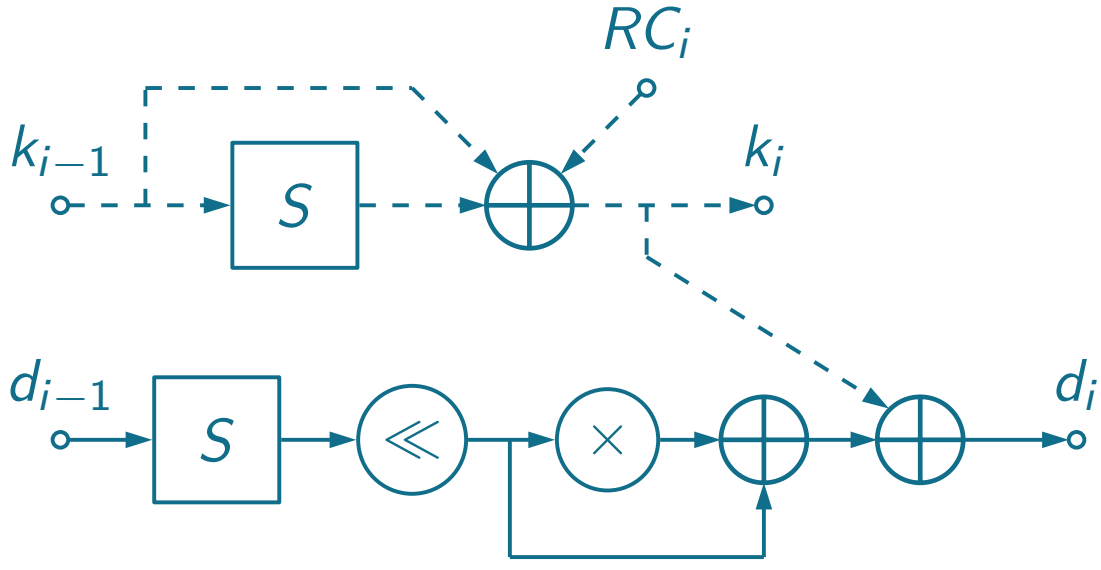
Latency: n ns **Throughput:** $\frac{1}{n}$ Gbit/s **Critical Path:** $\frac{1}{n}$ GHz

Synthesis Results

- Virtex 6 (`xc6vlx240t-2ff1156`)
- Xilinx ISE
  - Default synthesis settings
  - IOB-bonded top module
  - Unconstrained timing
  - No special resources (e.g. DSP slices)
- ASIC results are available in the paper



SP Network, 10 Rounds, 8-bit S-box



Size

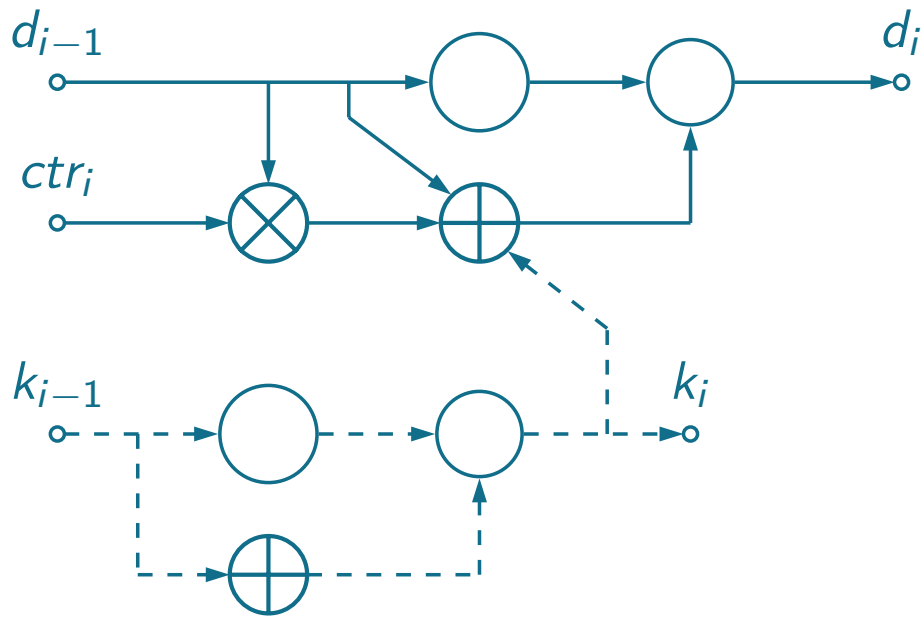
8,984 LUTs

Critical Path

24.7 ns

- Low number of rounds
- Big S-box

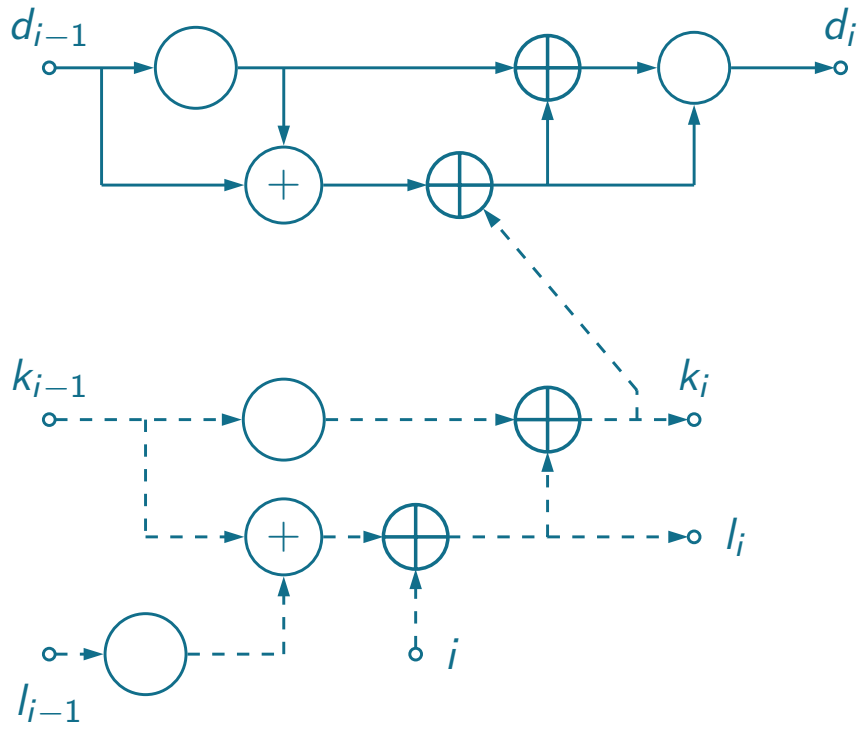
254 Rounds



Size
1,064 LUTs
Critical Path
41.2 ns

- Very small round function
- Large number of rounds

22 Rounds



Size

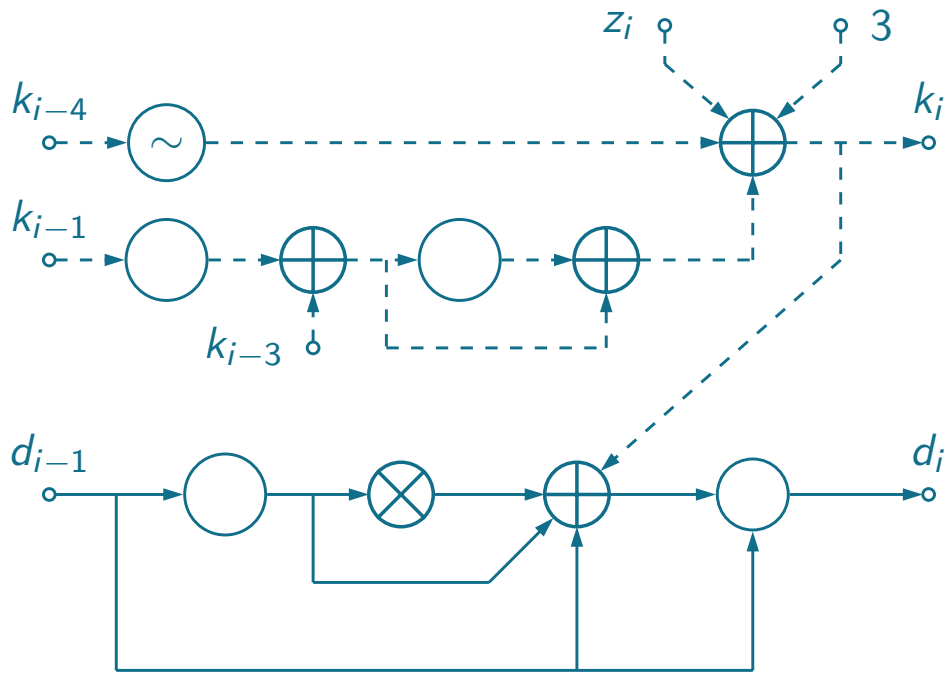
1,513 LUTs

Critical Path

40.3 ns

- Limited number of rounds
- Arithmetic addidition

Feistel Cipher, 32 Rounds



Size

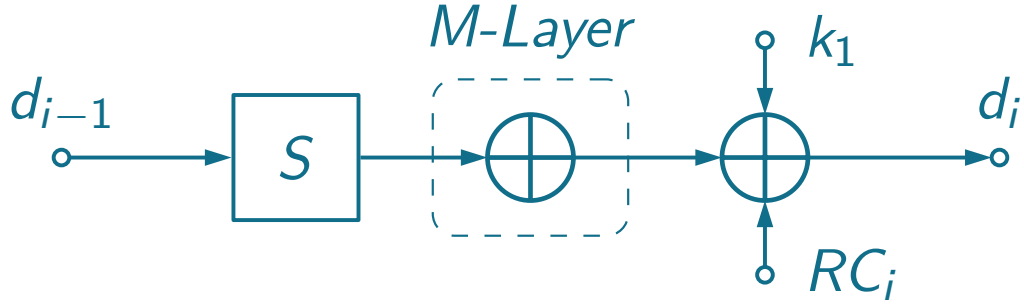
960 LUTs

Critical Path

20.4 ns

- Very small round function
- Limited number of rounds

Unrolled, 12 Rounds, 4-bit S-box, Matrix Layer



Size
1,244 LUTs
Critical Path
16.4 ns

- Low number of rounds
- Small S-box
- No key expansion
- Decryption can use same hardware

	Cipher	Size [LUTs]	Critical Path [ns]
32/64	SIMON	960	20.4
	SPECK	1,513	40.3
32/80	KATAN	1,064	41.2
64/80	KATAN	2,550	47.3
	PRESENT	2,089	29.2
	RECTANGLE	1,682	19.4
64/128	PRESENT	2,203	32.6
	PRINCE	1,244	16.4
	RECTANGLE	1,730	19.3
	SIMON	2,688	27.3
	SPECK	3,594	50.3
128/128	AES	8,984	24.7

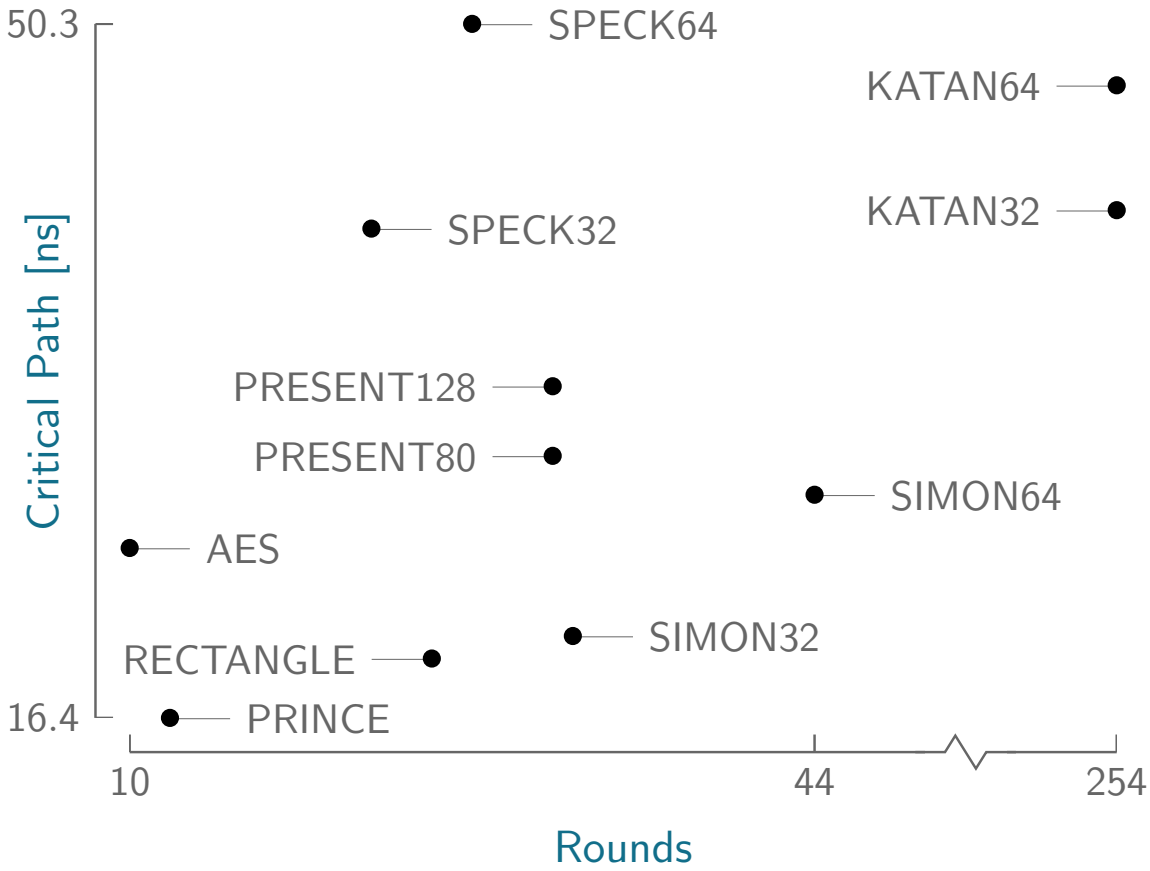
Comparison

	Cipher	Size [LUTs]	Critical Path [ns]
32/64	SIMON	960	20.4
	SPECK	1,513	40.3
32/80	KATAN	1,064	41.2
64/80	KATAN	2,550	47.3
	PRESENT	2,089	29.2
	RECTANGLE	1,682	19.4
64/128	PRESENT	2,203	32.6
	PRINCE	1,244	16.4
	RECTANGLE	1,730	19.3
	SIMON	2,688	27.3
	SPECK	3,594	50.3
128/128	AES	8,984	24.7

	Cipher	Size [LUTs]	Critical Path [ns]
32/64	SIMON	960	20.4
	SPECK	1,513	40.3
32/80	KATAN	1,064	41.2
64/80	KATAN	2,550	47.3
	PRESENT	2,089	29.2
	RECTANGLE	1,682	19.4
64/128	PRESENT	2,203	32.6
	PRINCE	1,244	16.4
	RECTANGLE	1,730	19.3
	SIMON	2,688	27.3
	SPECK	3,594	50.3
128/128	AES	8,984	24.7

Recommendations

- Start from an unrolled structure
- SP networks with small S-boxes
- Use boolean operations
- Limit the number of rounds



Conclusion

- PRINCE is confirmed to be the fastest, with competitive area
- For smaller block sizes, SIMON also performs well
- Latency of most ciphers is too high for practical applications

- PRINCE is confirmed to be the fastest, with competitive area
- For smaller block sizes, SIMON also performs well
- Latency of most ciphers is too high for practical applications

Questions?

pieter.maene@esat.kuleuven.be