KU LEUVEN

Iterating Von Neumann's Post-Processing under Hardware Constraints

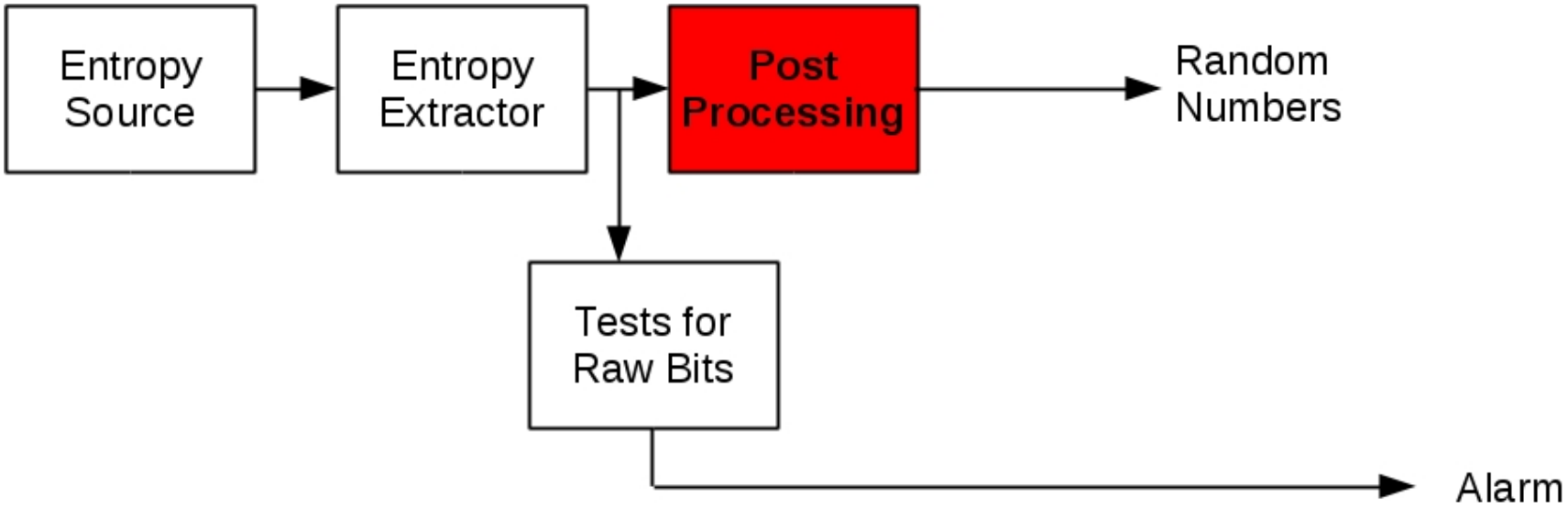
Vladimir Rožić, Bohan Yang, Wim Dehaene and Ingrid Verbauwhede

HECTOR

Outline

- Background
  - True Random Number Generators (TRNG)
  - Von Neumann's (VN) post-processing
  - Iterating Von Neumann's (IVN) post-processing
- Goals
- Optimization
- Verification
- Conclusions

True Random Number Generators



Von Neumann's Post-processing

- Completely removes bias
- Reduces throughput
  - EXAMPLE:

    100 Mb/s

    10% bias

    Shannon Entropy: 97.1 Mb/s

    24 Mb/s after VN

    73.1 Mb/s of entropy wasted

S	S_{VN}
00	-
01	1
10	0
11	-

Iterating Von Neumann's Post-processing

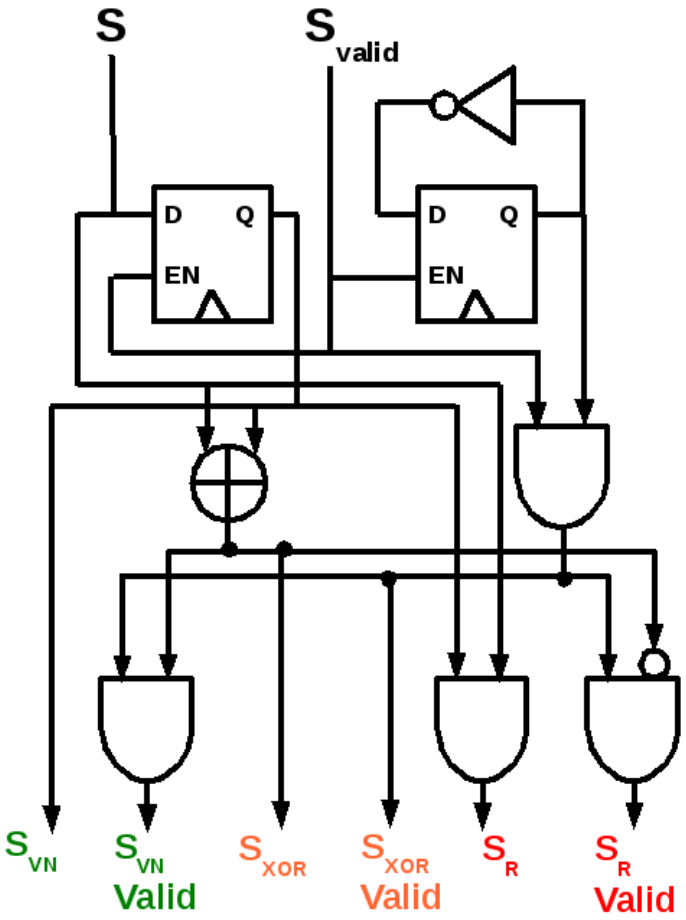
															bias	*Shannon Entropy per bit*	Throughput [Mbps]
S	0 1	1 1	1 1	0 1	1 0	1 1	1 1	1 0	0 1	0 1	0 0	0 0	1 0	1 1	*10%*	*0.971*	*100*
S_{VN}	1			1	0			0	1	1			0		0%	1	24
S_{XOR}	1	0	0	1	1	0	0	1	1	1	0	0	1	0	2%	0.9988	50
S_R		1	1			1	1				0	0		1	19.23%	0.8905	26

[5] Y. Peres, “Iterating Von Neumann's Procedure for Extracting Random Bits,” *Ann. Statist.* Vol. 20, no. 1. pp. 590-597, 1992.

Goals

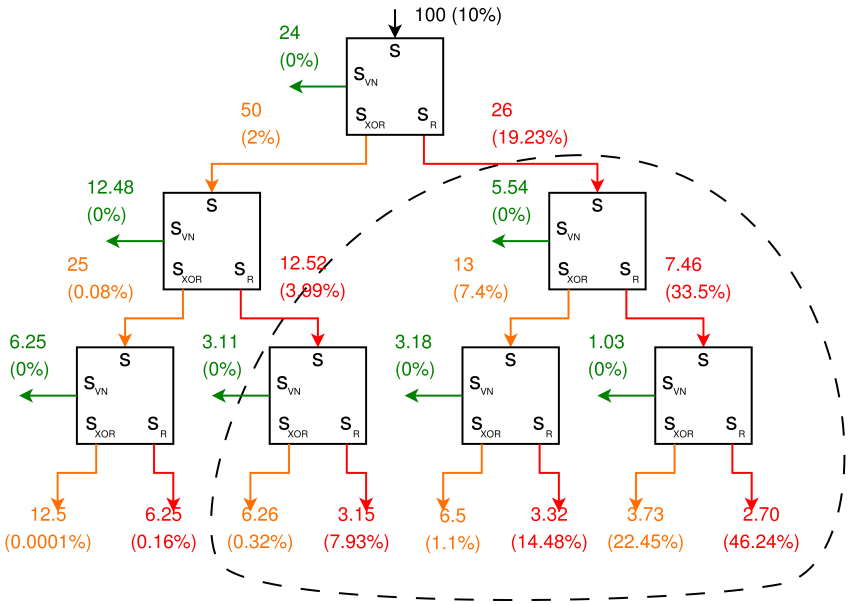
- IVN under hardware constraints
    - Limited area
    - Limited computation time
    - Interface
- Optimal post-processing structure
    - Bias
    - Max. area

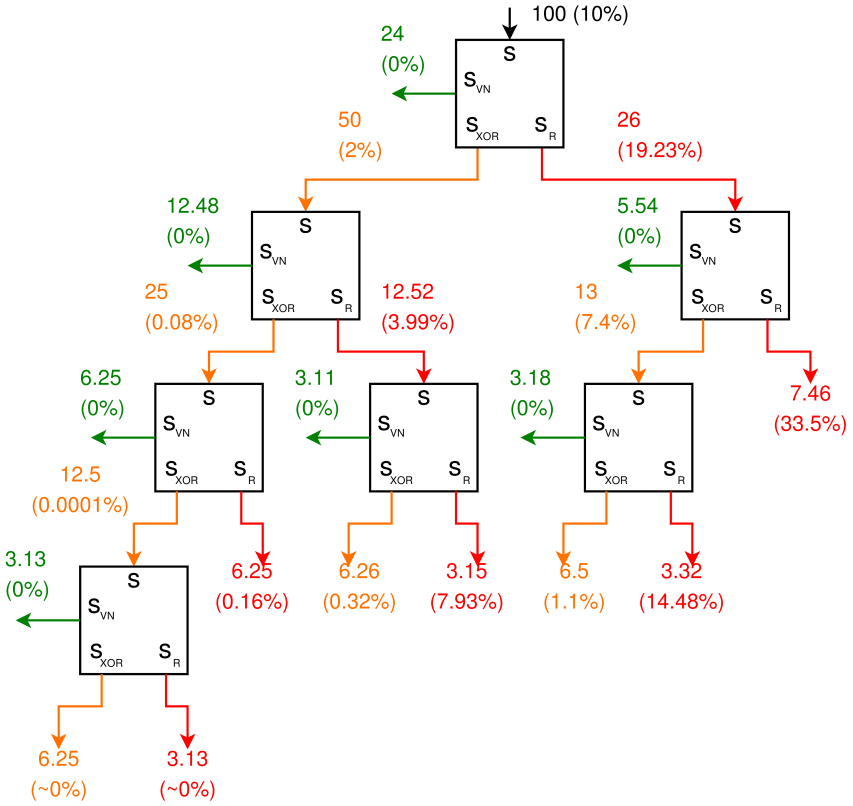
Elementary IVN Operation



S	S_{VN}	S_{XOR}	S_R
00	-	0	0
01	1	1	-
10	0	1	-
11	-	0	1

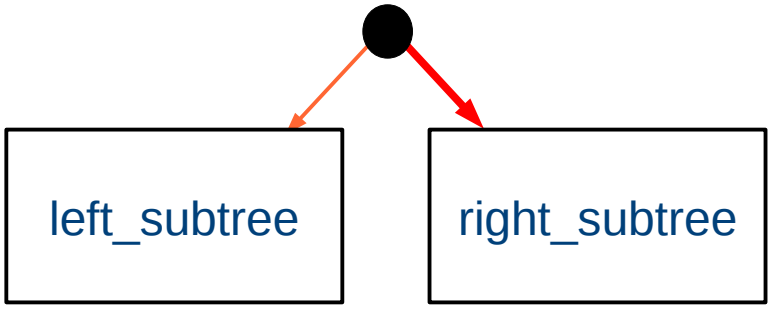
Examples





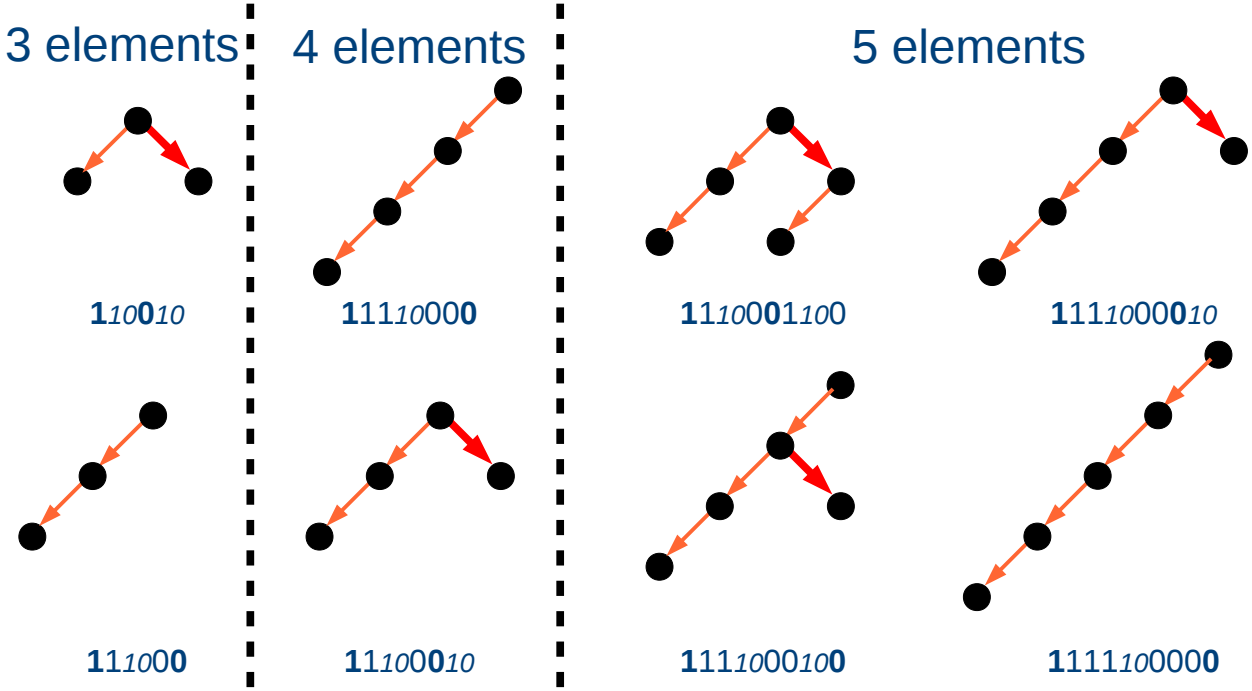
KU LEUVEN

Binary Trees Notation



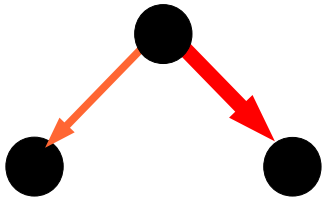
1 <left_subtree> **0** <right_subtree>

Binary Trees



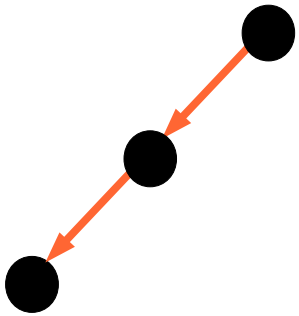
KU LEUVEN

3-element Structures



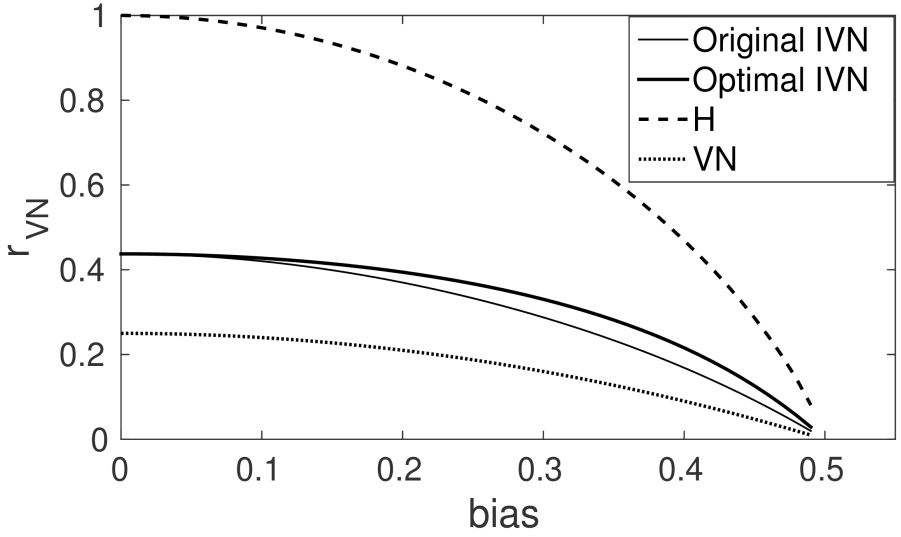
65.67 GE
0.29 ns

1*10***0***10*



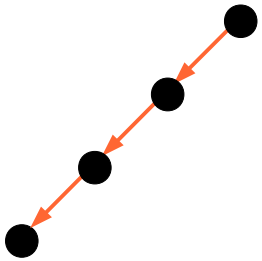
65 GE
0.27 ns

11*10***0****0***



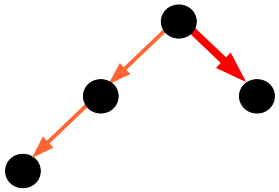
KU LEUVEN

4-element Structures



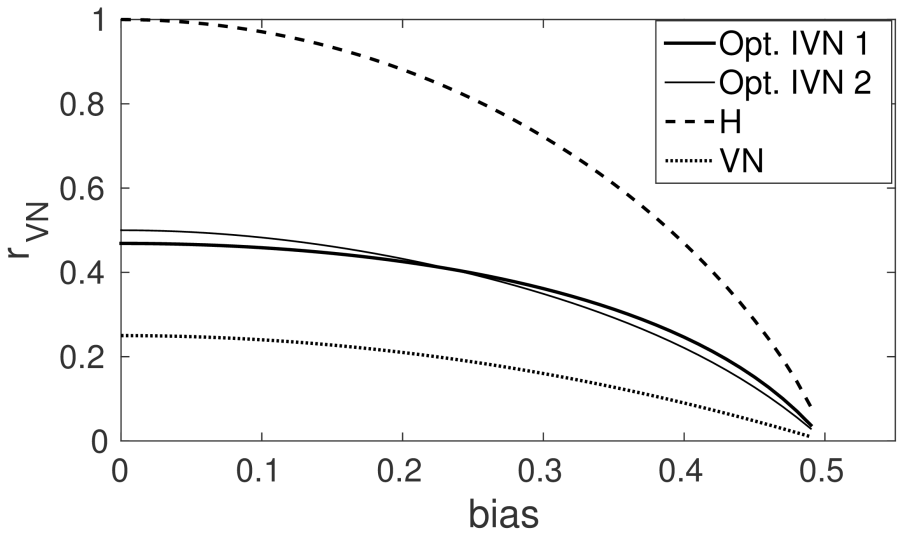
1111*0*000**0**

84.67 GE
0.36 ns



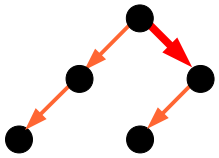
11*1*00**0***10*

87 GE
0.36 ns



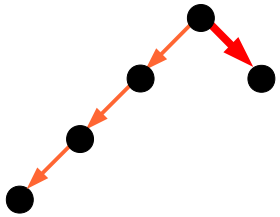
KU LEUVEN

5-element Structures



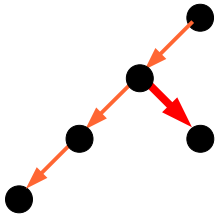
11*10*0**0**1*10*0

109.33 GE,
0.31 ns



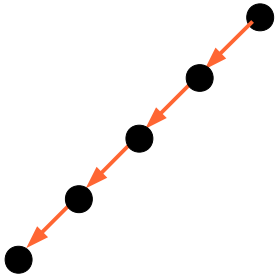
1111*0*000**0***10*

109.67 GE,
0.4 ns



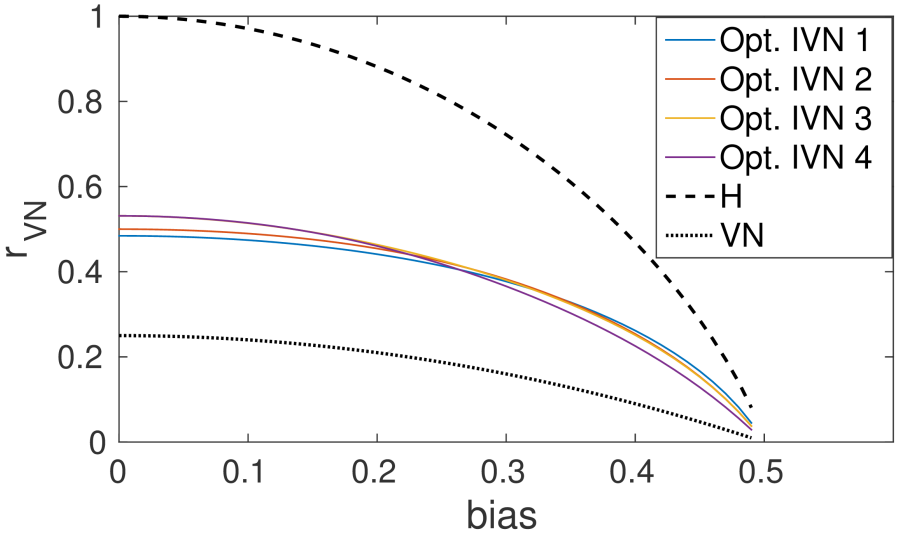
1111*0*000*10***0**

109 GE,
0.46 ns



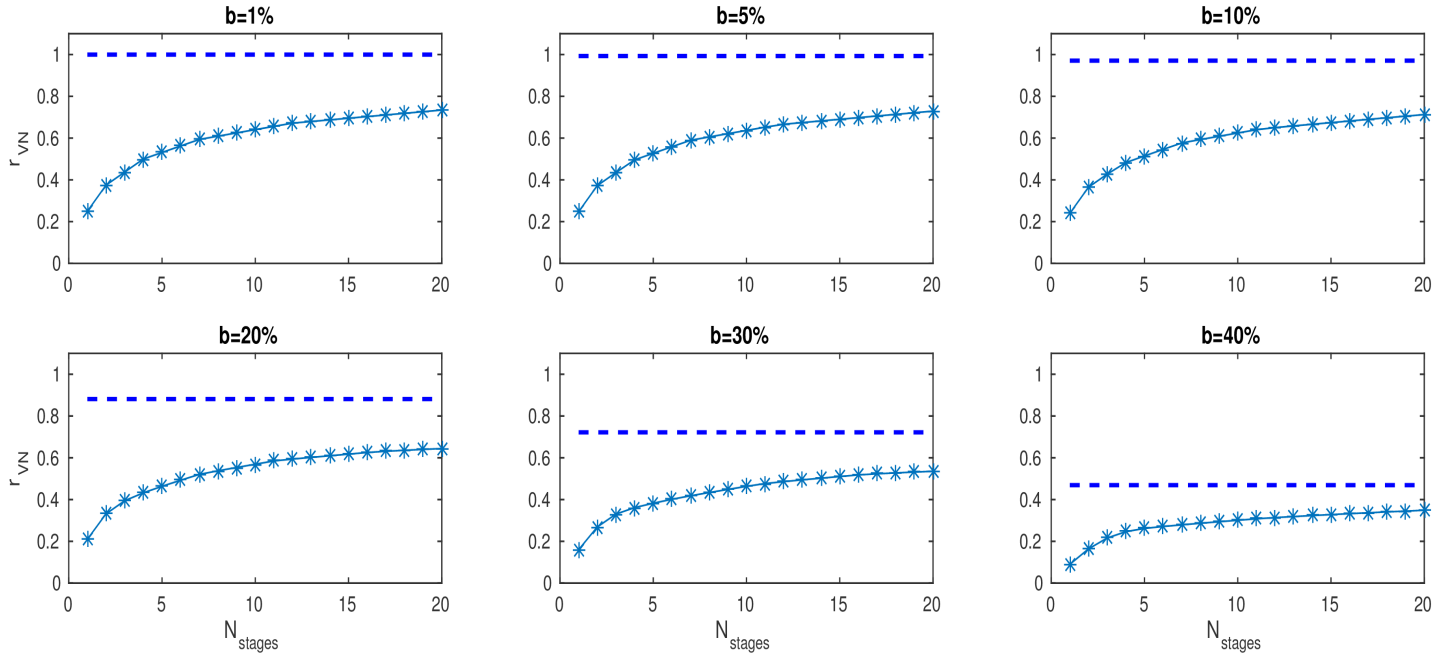
11111*00*000**0**

107 GE,
0.45 ns



KU LEUVEN

Throughput Efficiency



KU LEUVEN

Verification

Bias [%]	r_{VN} [%]					
	3 elements		4 elements		5 elements	
	Comp.	Meas.	Comp.	Meas.	Comp.	Meas.
12.5	42.14	42.07	47.31	47.2	50.47	50.3
25	36.69	36.69	39.82	39.7	42.63	42.4
37.5	35.11	25.22	28.2	28	29.76	29.8

Conclusions

- Optimal post-processing depends on the bias
- Algorithm for finding optimal structure at design-time
- VN limitations still apply
- 5-element structures always extract more than 50% of the available entropy

Questions?

KU LEUVEN