Does gate count matter? Hardware efficiency of logic-minimization techniques for cryptographic primitives

Shashank Raghuraman and Leyla Nazhandali

Lightweight Cryptography Workshop 2019

Acknowledgement

We would like to thank NIST for having funded this project.

Overview

- Motivation
  - Logic Minimization
  - Technology Cost Factors
- Evaluation Methodology
- Impact of Logic Synthesis
  - AES SBox
  - Polynomial Multiplier
  - Integrated Design Example
- Conclusion

Motivation

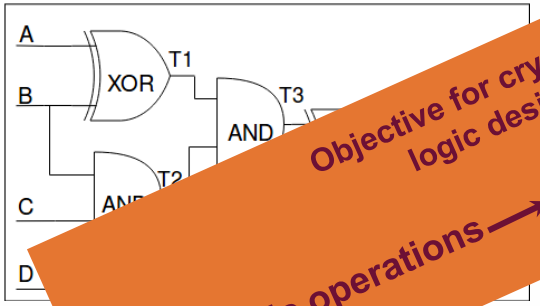
Efficiency of Logic Minimization Techniques for Cryptographic Hardware

Constant search for smaller crypto-hardware

- Proliferation of embedded smart devices for the Internet-of-Things.
- Entire device is required to
  - Fit in a small form factor.
  - Be energy-efficient.
- Small area budget for security.

Boolean Representation of a Cryptographic Function

```
T1 = A ^ B
T2 = B & C
T3 = T1 & T2
T4 = T3 ^~ D
S = T2 & T4
```



Objective for cryptographic logic designers

Fewer logic operations → Fewer hardware gates

- d as AND/XOR/NOT
- timate of hardware as mpared to abstract input-output relationship.
- Easy to factor out redundant sub-expressions.

Expectation

Fewer logic gates

↓

Smaller hardware

Low Gate Count (LGC) circuits

Specialized Tools to minimize gate count

Gate count used to compare crypto designs

tional architectures. To the authors knowledge the gate count of 48 AND/62 XOR is the lowest one reported in technical literature for

scheme using a smaller number of AND and XOR gates than in known schemes, although maintaining a comparable time delay.

For matrix U, the smallest circuits we found had 23 $\oplus$ gates. Among the many such circuits, the shortest ones have depth 7. It is worthwhile

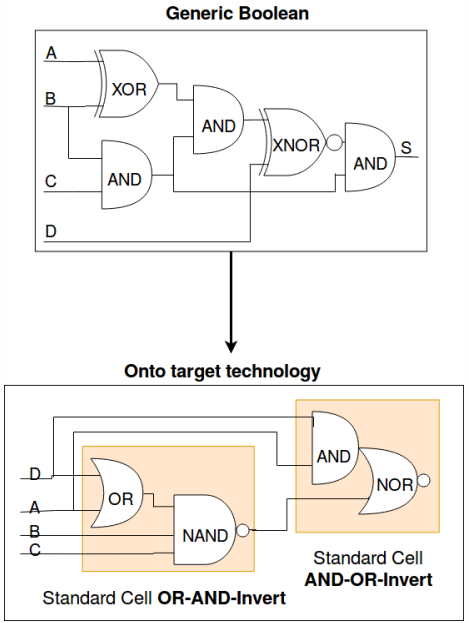
timal implementation. Here, the efficiency of the multiplication is measured in terms of the number of XOR operations needed to implement the multiplication. While our results are potentially of larger interest, we

- **Record-setting gate count for cryptographic primitives.**
- **Cost function**
  Gate count or logical depth
- **Designed by Boyar, Peralta et al.**

Efficiency of Logic Minimization Techniques for Cryptographic Hardware

Boolean Logic to hardware

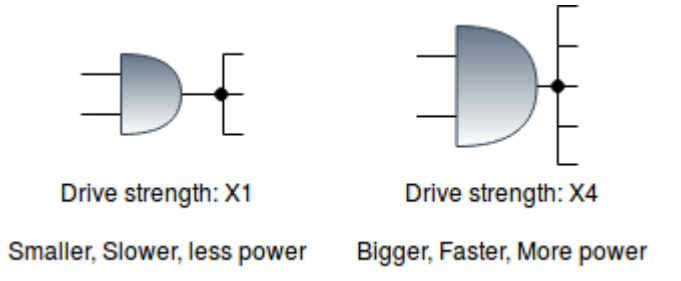
- Logical expressions are mapped onto a library of “standard cells”.



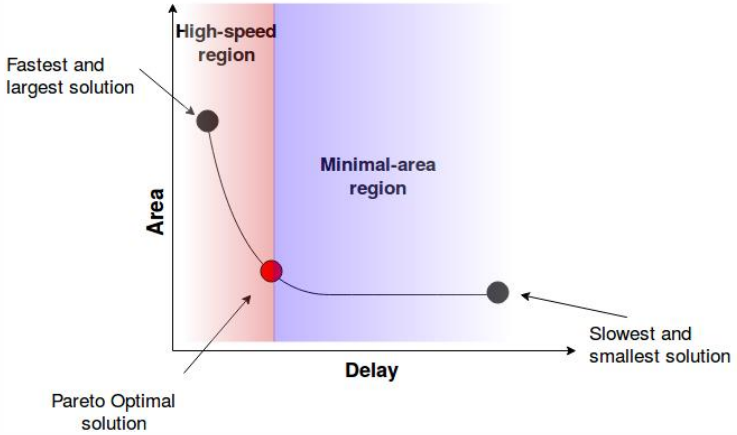
- Many possible hardware solutions for a single Boolean expression.
- Choosing the final design is driven by trade-offs between technology cost factors.

Technology Cost Factors

- Each cell incurs non-zero **Delay** before its output reflects a change in inputs.
- Each cell comes with a specific **Drive Strength**, i.e. ability to drive logic at its output.
- Area and Power efficiency often come at the expense of performance.



Typical Area-delay trade-off

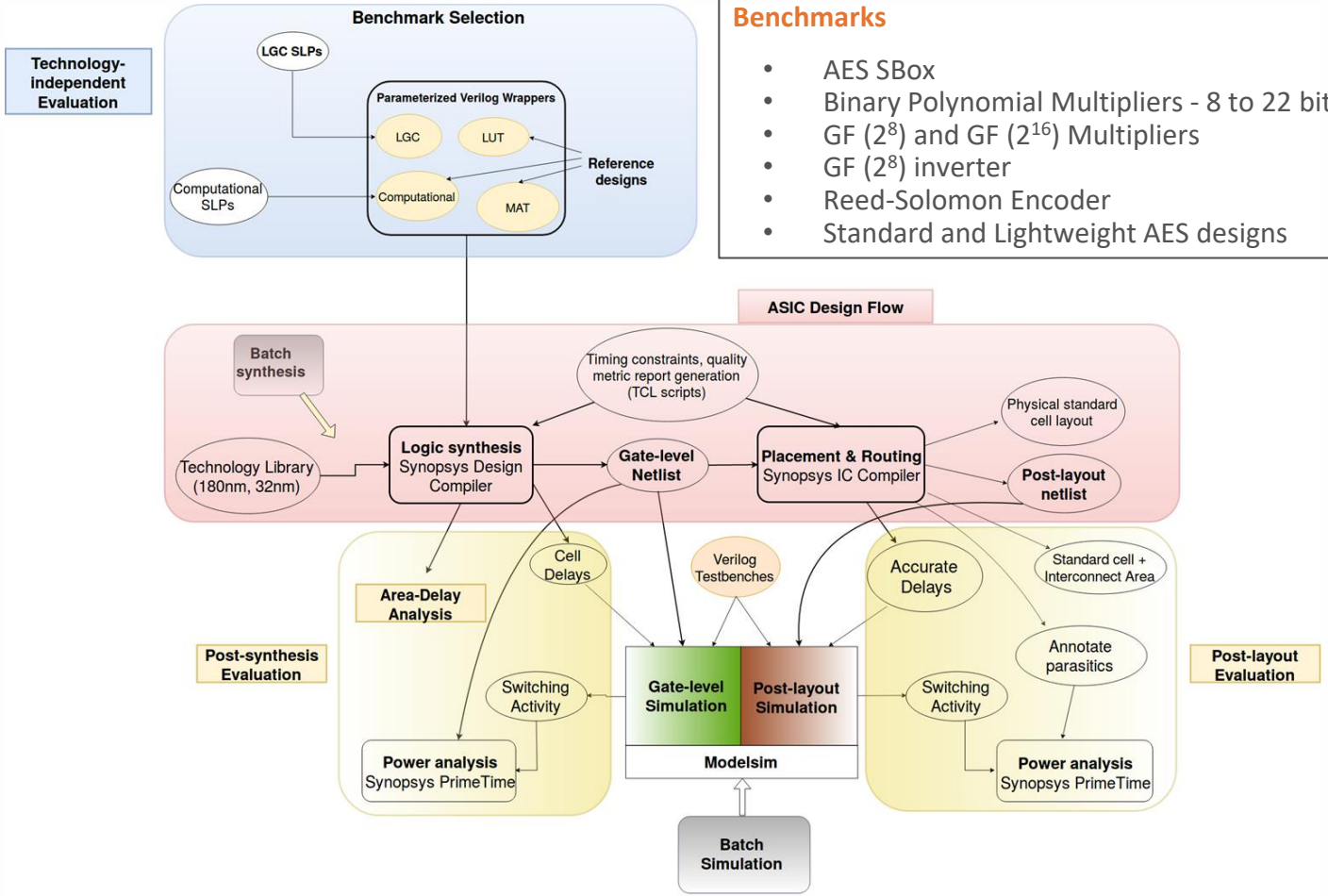


Our Contributions

- Circuit-level analysis of low-gate-count (LGC) circuits
  - Evaluation of LGC designs with widely-used benchmarks for same function, including abstract and algebraically minimized versions.
  - Factor the area-performance trade-off -comparing alternatives over multiple frequencies.
  - Analyze the impact of ASIC implementation flow on LGC circuits.
    - Technology-independent - Gate count
    - Post-synthesis - Impact of logic transformation and mapping
    - Post-layout - Impact of physical design

Evaluation of logic-minimized circuits

Analysis Methodology



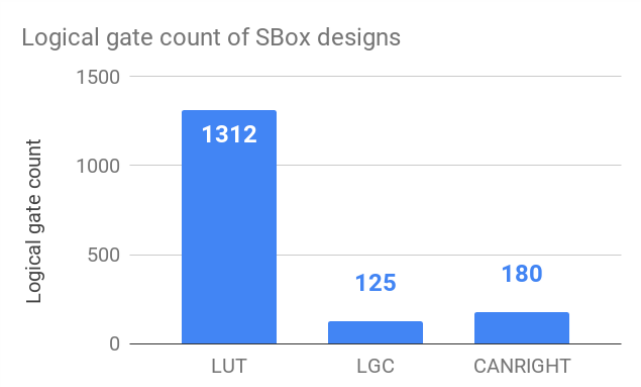
Benchmarks

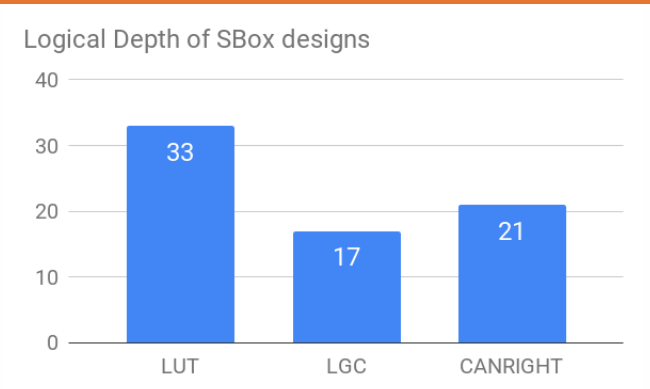
- AES SBox
- Binary Polynomial Multipliers - 8 to 22 bits
- GF (2^8) and GF (2^{16}) Multipliers
- GF (2^8) inverter
- Reed-Solomon Encoder
- Standard and Lightweight AES designs

Step 1: Analyzing the Impact of Logic Synthesis

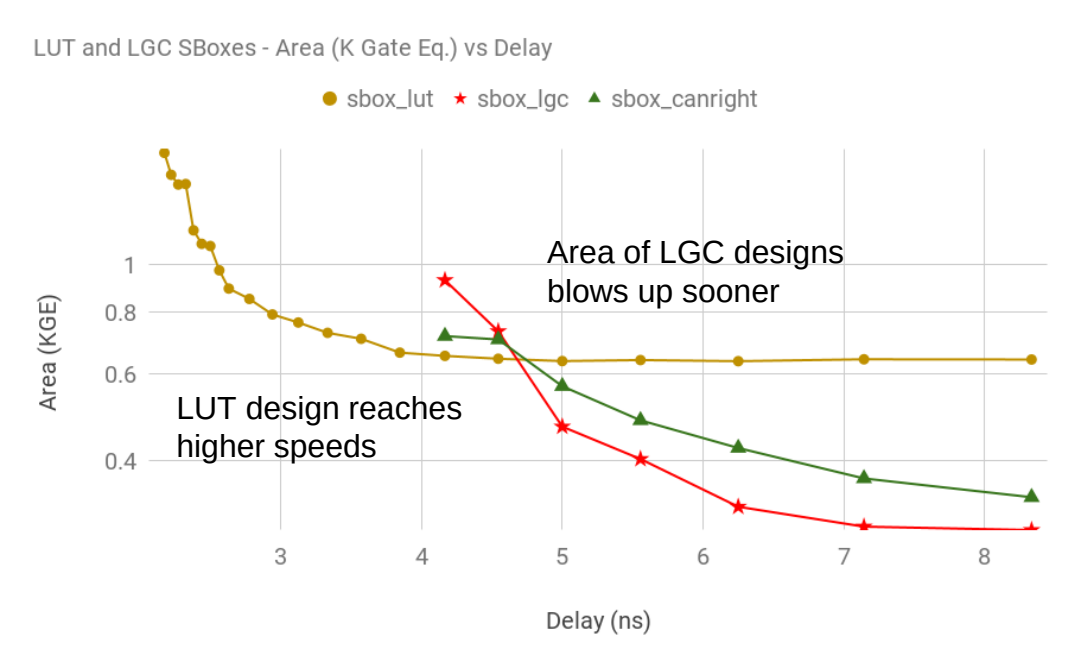
- Benchmark 1 : AES SBox
- Design Alternatives
  - Look-Up Table
  - Canright SBox - Compact SBox using algebraic simplification
  - LGC SBox - Minimized by LGC tool
- Technology-independent Comparison

LUT appears to be larger (more gates) and slower (more logic levels).





Post-synthesis Area of SBox designs

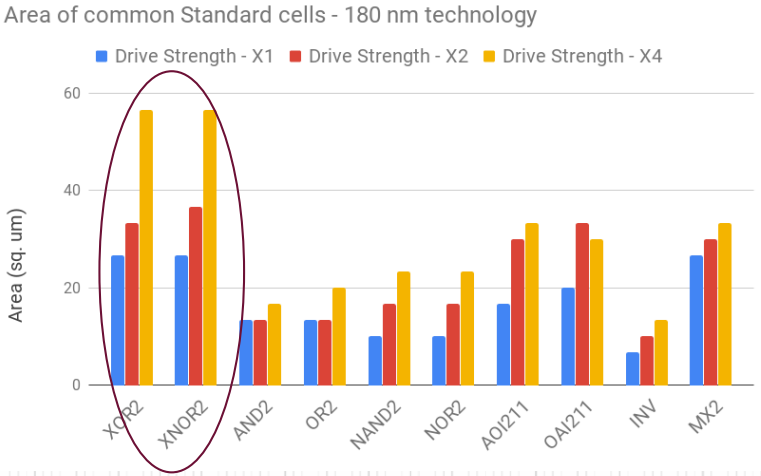


	LGC *vs* LUT	LGC *vs* Canright
Minimal-Area	**50%** smaller	**20%** smaller
High-Speed	**40%** larger	**25%** larger

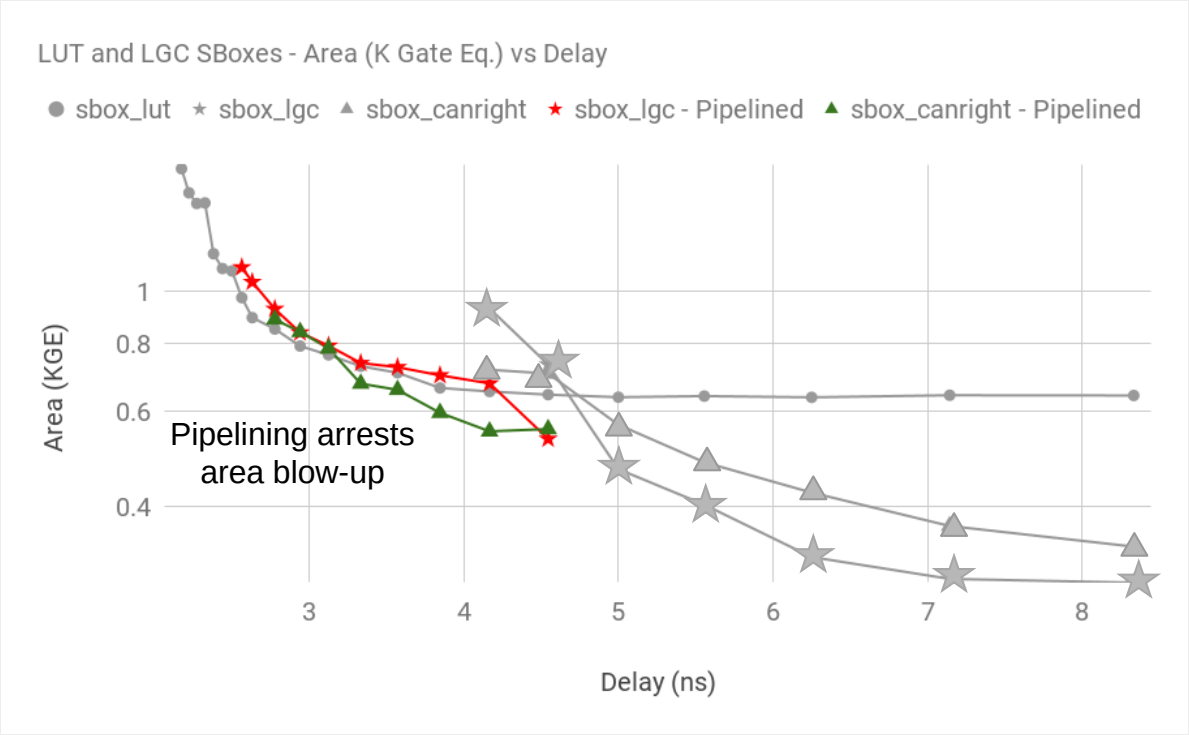
- **Abstract LUT SBox is easily collapsed into fewer levels of gates on hardware.**
  - **LUT: 33 levels (initial) → 14 (post-synthesis)**
  - **LGC: 17 levels (initial) → 18 (post-synthesis)**

Fewer, smaller cells on critical path of LUT SBox.

- **High XOR-dominance of LGC SBox**
  - XOR cell is 2-2.5x bigger than other cells.

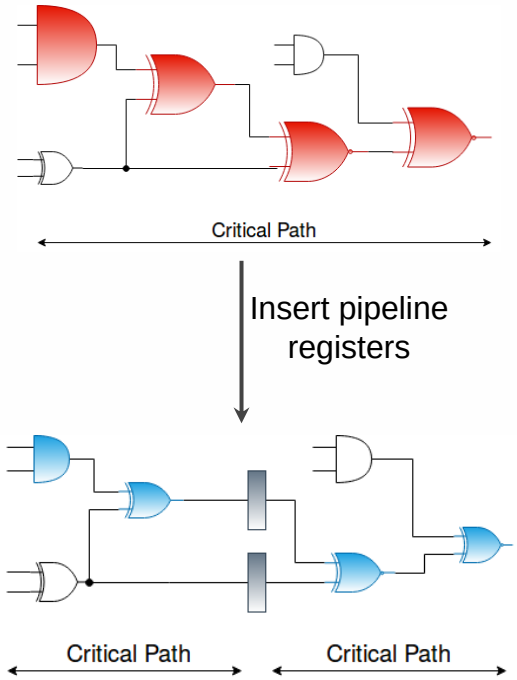


Post-synthesis Area of SBox designs

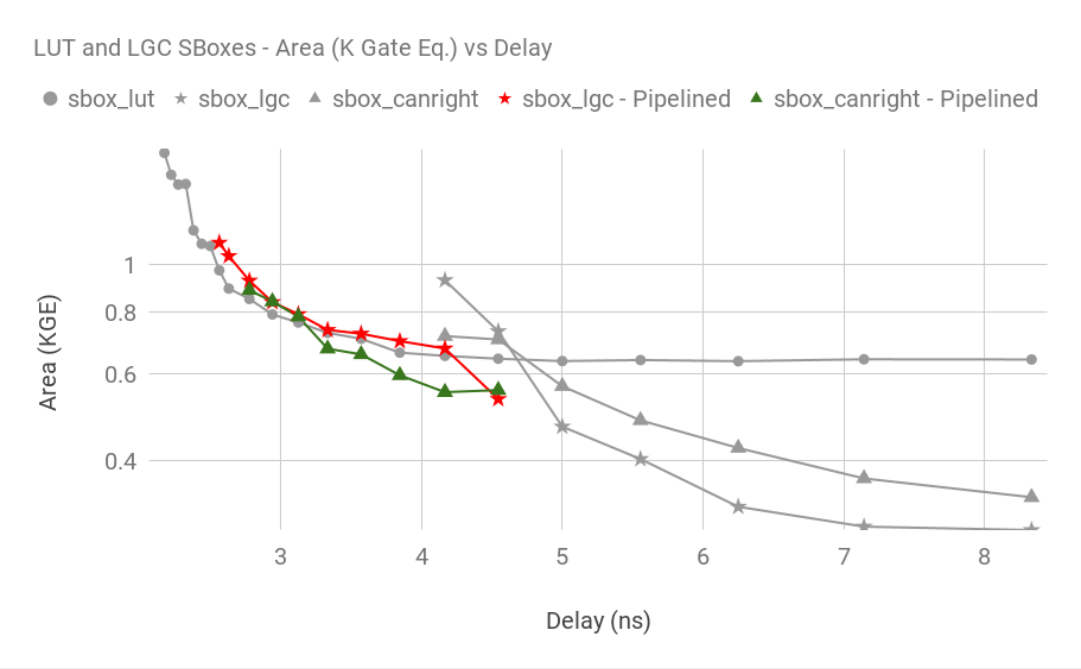


Inserting a pipeline stage

- Pipelining shortens critical path.
  - Easier to meet timing.
  - Cells can be smaller.



Post-synthesis Area of SBox designs

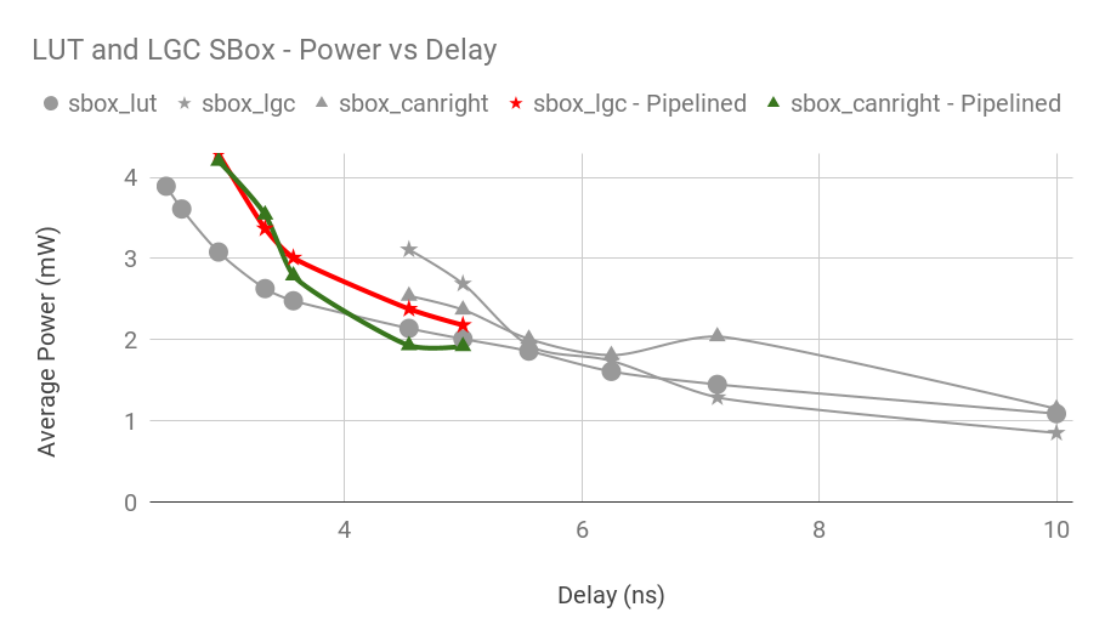


Observations

- Smaller fanout per gate ⟶ Smaller increase in area after pipelining.
- LGC designs - Small fanout per gate.
  - LGC : ~1.7
  - LUT : ~2.5

	LGC *vs* LUT	LGC *vs* Canright
Minimal-Area	**50%** smaller	**20%** smaller
High-Speed	**40%** larger	**25%** larger
High-Speed (with pipeline)	**± 15%**	**10-15%** larger

Post-synthesis Power of SBox designs



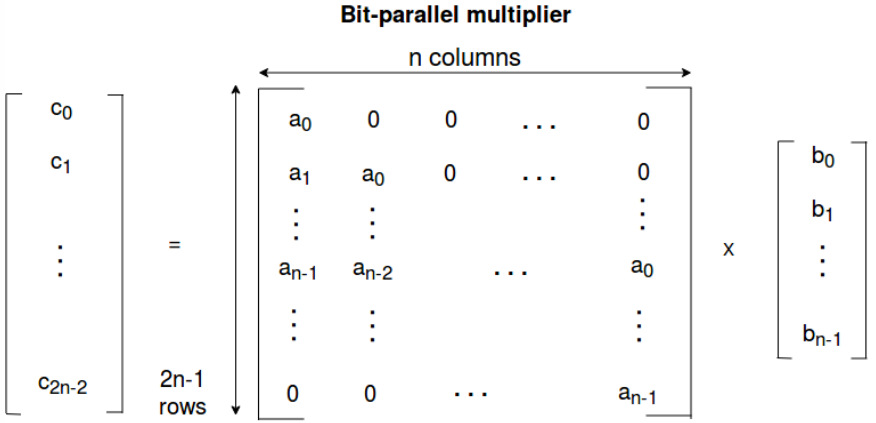
	LGC *vs* LUT	LGC *vs* Canright
Minimal-Area	**15-20%** lower	**30%** lower
High-Speed	**30-45%** higher	**15-20%** higher
High-Speed (with pipeline)	**20-30%** higher	**10-20%** higher

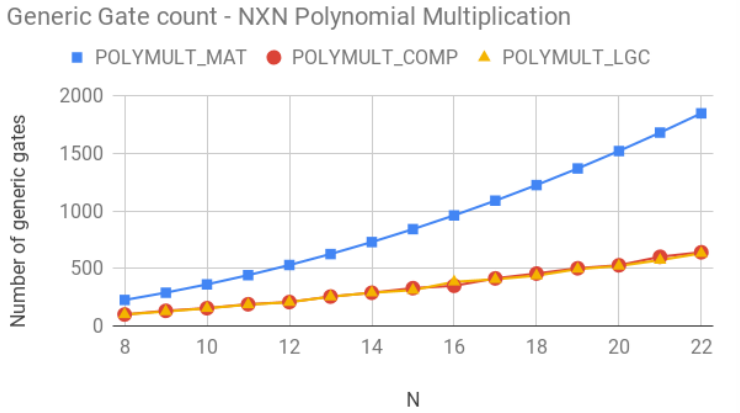
- **LUT SBox is more power-efficient.**
- **Pipelining LGC SBox does not improve its power-efficiency.**

Smaller area or fewer gates does not imply lower power.

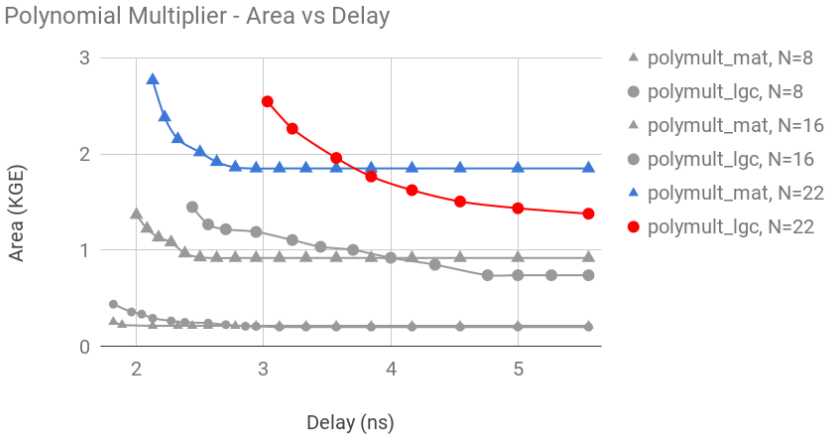
Impact of Logic Synthesis

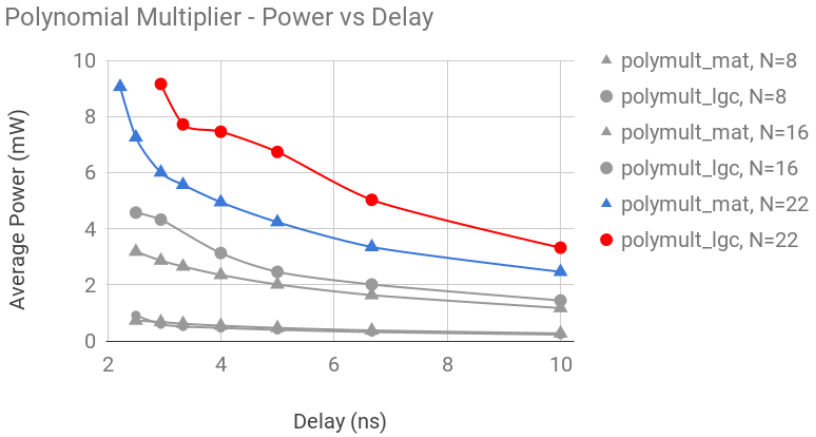
- Benchmark 2 : Binary Polynomial Multiplier
- Design Alternatives
  - Matrix-Multiplier
  - LGC Multiplier - Minimized by LGC tool
- Technology-independent Comparison





Post-synthesis area and power of Polynomial Multipliers



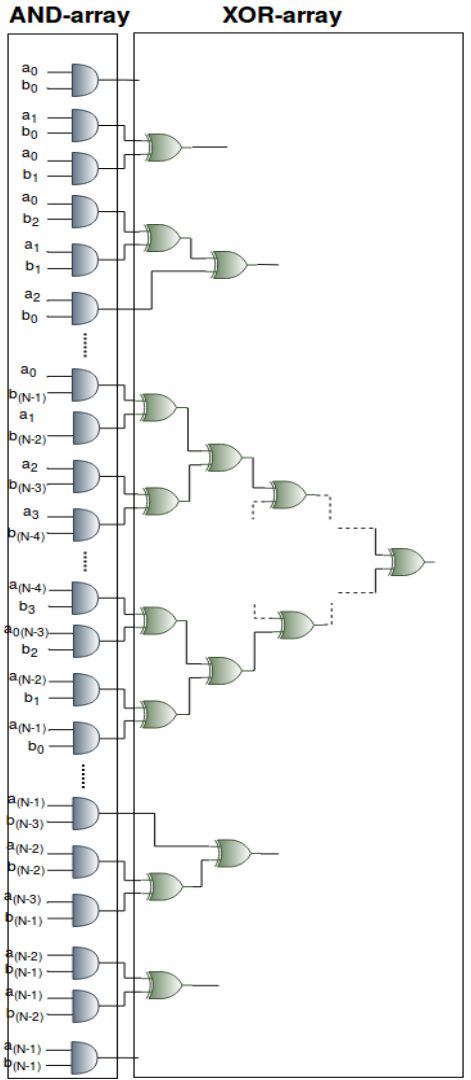


- **Area-efficiency of LGC multipliers is lost at high speeds, and the difference worsens with increase in N.**
- **Power-efficiency of LGC multipliers is lost for all N > 14, regardless of speed.**

In short, a matrix multiplier "scales" better with multiplier size.

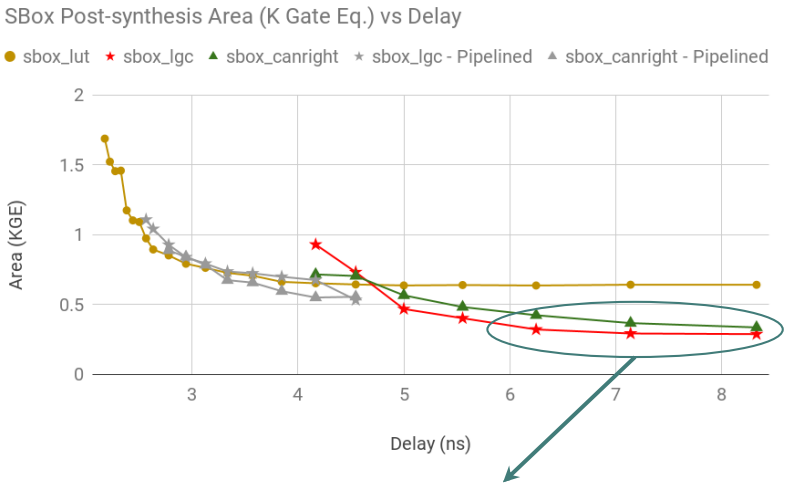
Regularity in structure of a matrix multiplier

- Area Efficiency
  - Symmetric and regular structure - easily collapsed into fewer levels during optimization.
  - Effect of optimization more pronounced with increase in speed and multiplier width.
- Power Efficiency
  - Both Matrix and LGC multipliers are XOR-dominant, but matrix is power-efficient due to more balanced gate delays.

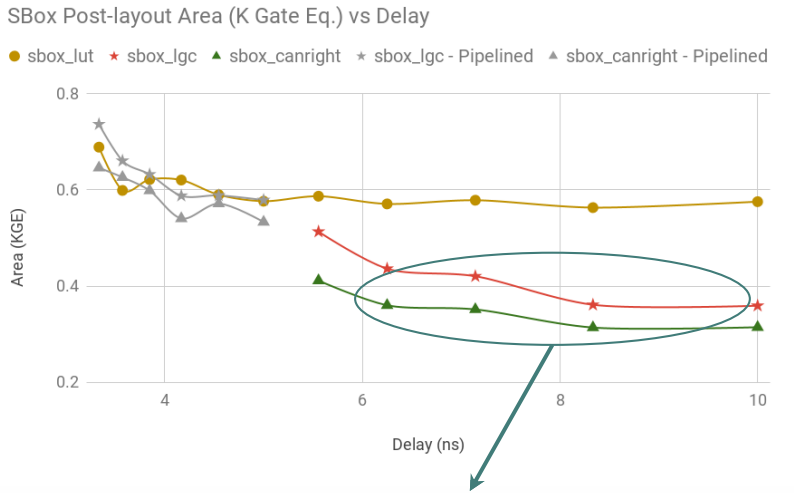


Step 2: Impact of Physical Design

- For large differences in logical gate count, differences in post-layout area of circuits closely follows those of their post-synthesis versions.
- When designs have small differences in gate count, post-synthesis results are liable to be flipped.
- Examples: LGC and Canright SBox, LGC and Matrix multipliers for small N.



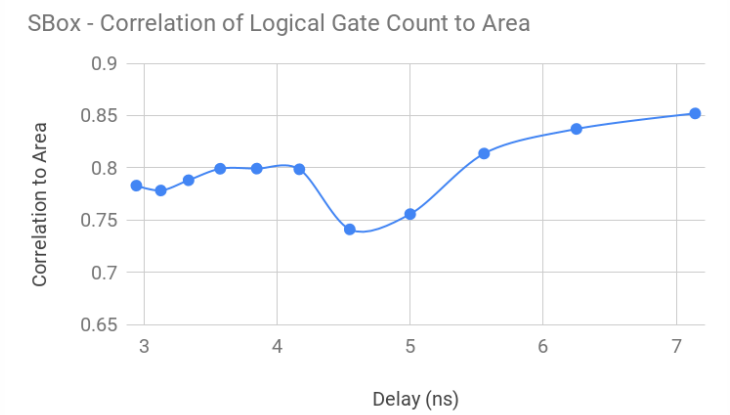
After synthesis - LGC 20% smaller than Canright

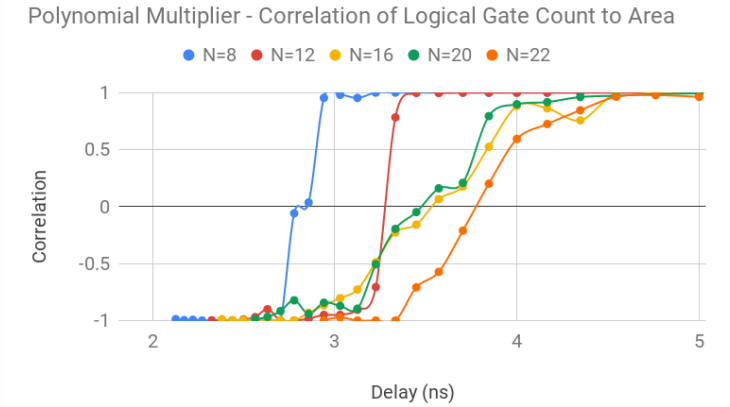


After place&route - LGC 20% bigger than Canright

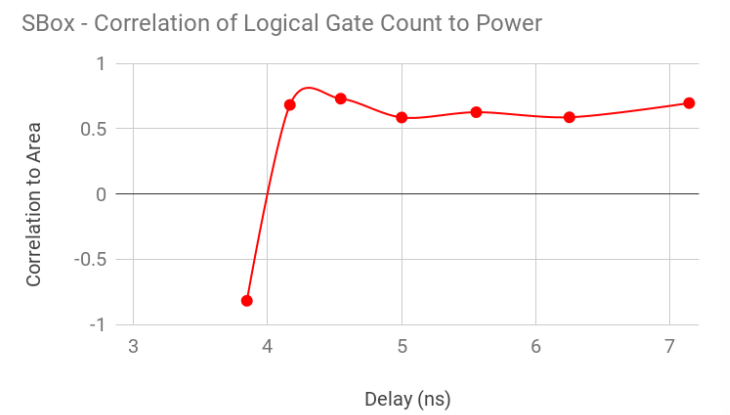
How well are logical metrics related to hardware quality metrics?

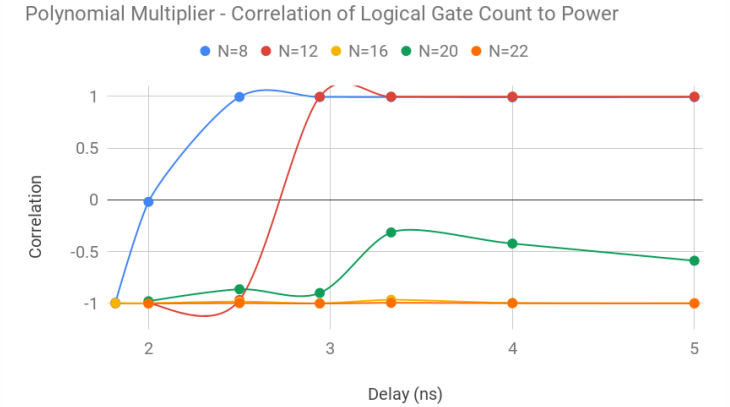
Correlation of logical gate count to hardware area.





Correlation of logical gate count to power.

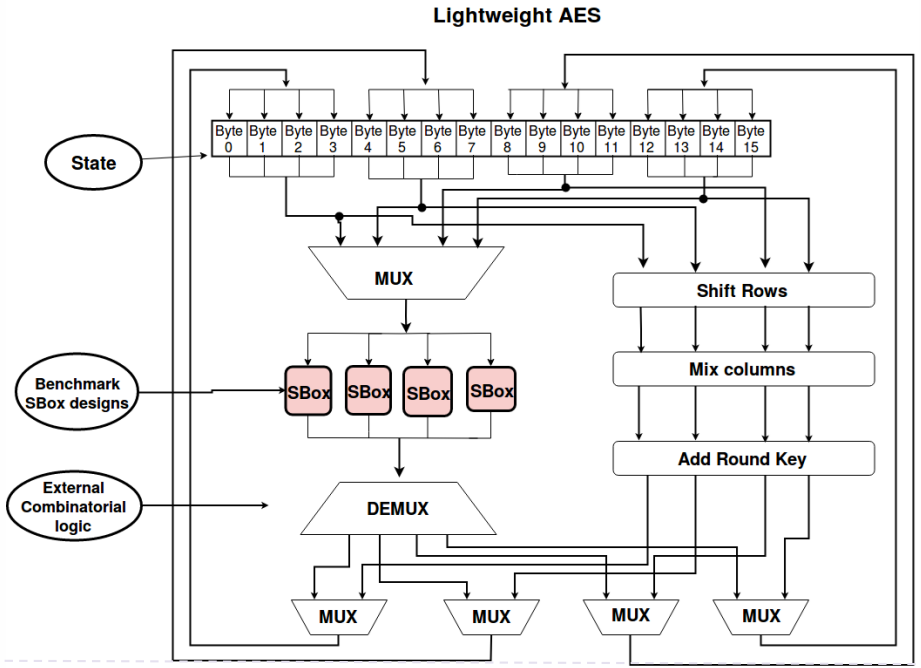




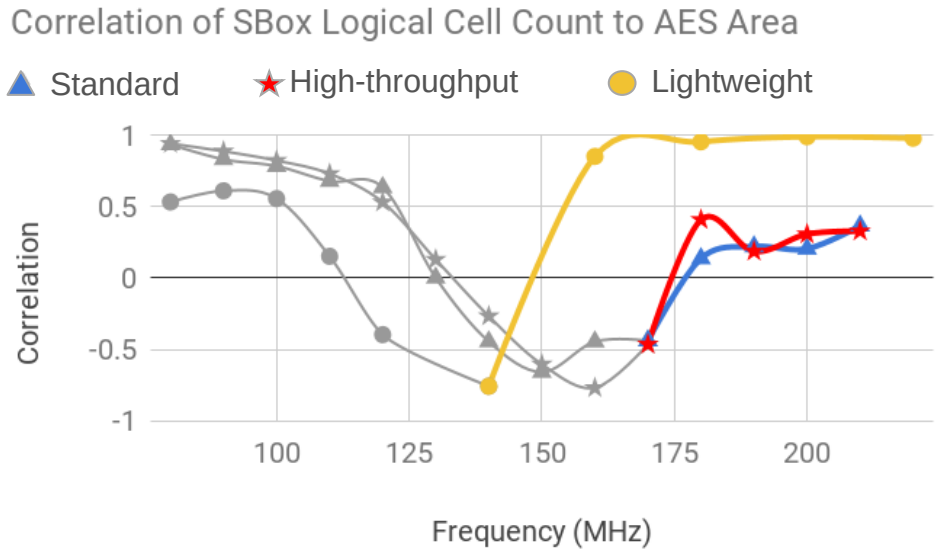
Integrated Design Example

- Different SBox circuits integrated into AES designs
  - Demonstrate impact of logical-minimization in practical context.
  - Effect of combined optimization of crypto-primitive with external logic.

- AES Design Alternatives
  - Standard Version
    - SBox for each byte of State and Key Expansion - 20 SBoxes in total
  - High-throughput
    - Two AES rounds in single cycle - 40 SBoxes in total
  - Lightweight
    - Shared SBoxes - 4 in total



Post-synthesis Area of AES designs



At high frequencies, correlation increases due to effects of pipelining LGC designs.

Region	AES Type	LGC *vs* LUT	LGC *vs* Canright
Minimal-Area	Standard	12-32% smaller	7-13% smaller
	High-Throughput	18-33% smaller	5-13% smaller
	Lightweight	8% smaller	4-8% smaller
High-Speed	Standard	9-16% smaller	6-14% smaller
	High-Throughput	11-19% smaller	1-7% smaller
	Lightweight	9% smaller	± 5%

- **Comparison of cryptographic primitives requires context.**
- **Benefits of LGC SBox diminish for a lightweight version of AES.**

Summary of correlation analysis

Logical Metric	Design		Min-area Region		High-Speed Region	
			Area	Power	Area	Power
Gate Count	SBox		H	M	M	L
	Polynomial Multiplier	N ≤ 14	H	H	L	L
		N > 14	H	L	L	L
	GF Multiplier		M	M	L	L
	GF Inverter		M	M	L	L
	AES	Standard	H	L	L --> M	H --> L
		High-throughput	H	L	L --> M	M
		Lightweight	M	L	L --> H	H
Logical Depth	SBox		M	L	L	L
	Polynomial Multiplier	N ≤ 14	L	L	H	H
		N > 14	L	H	H	H
	GF Multiplier		H	H	H	H
	GF Inverter		L	L	M	L --> M
	AES	Standard	H	L	L --> M	H --> L
		High-throughput	H	L	L --> M	M
		Lightweight	M	L	L --> H	H

H - High correlation (>0.8)

M-Moderate Correlation(0.5-0.8)

L-Low Correlation (<0.5)

→ indicates change in level of correlation

Conclusions from analysis of combinatorial primitives

- Conduciveness of a design to logic optimization is not well-quantified by logical metrics.
  - Abstract designs are more flexible towards optimization.

- Use of logical metrics to estimate hardware quality depends on circuit speed.
  - Low Speed - Logical gate count is a good predictor of area only.
  - High speed - There is no correlation between gate count and hardware quality.

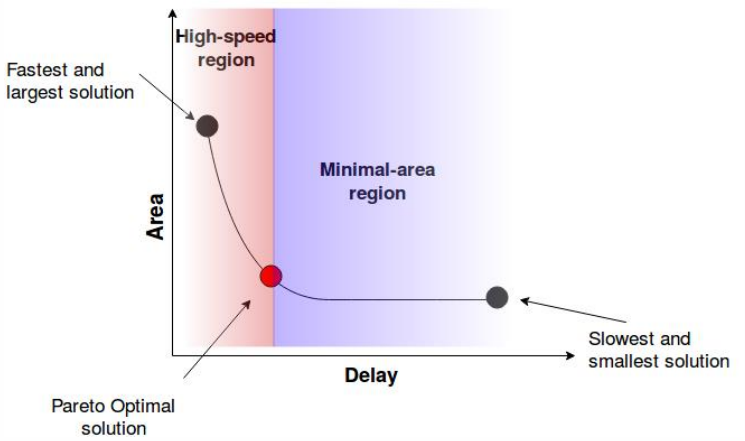
Thank you!

Backup Slides

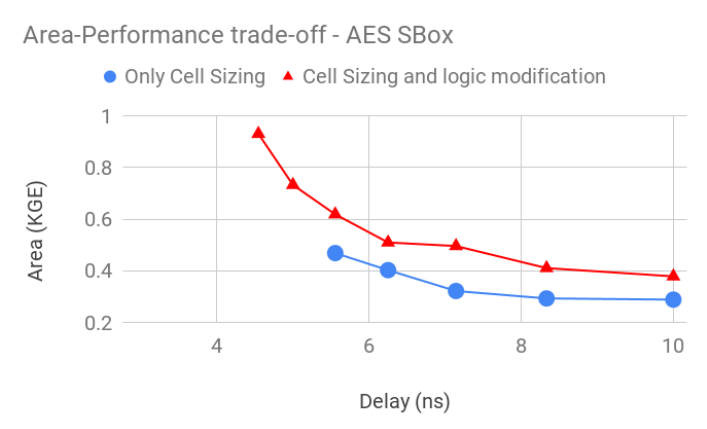
Technology Cost Factors

- Area and Power efficiency often come at the expense of performance.

Typical Area-delay trade-off



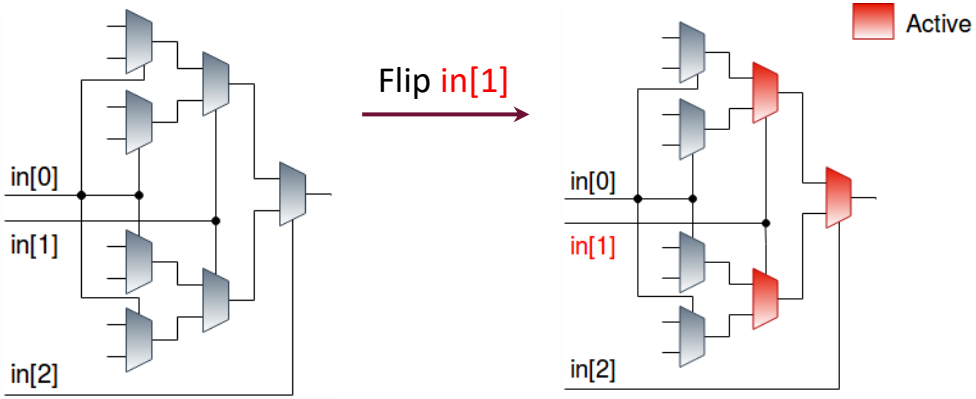
Area-delay trade-off present due to both “sizing” and logic modification.



Reasons for lower power-efficiency of LGC SBox

- 2.5x more cells in LUT SBox, but only 5-10% more toggles per computation. Why?

ROM-structure of LUT SBox results in few active cells per computation.



XOR gates are transparent to dynamic hazards.

A	B	Y
~A	B	~Y
A	~B	~Y

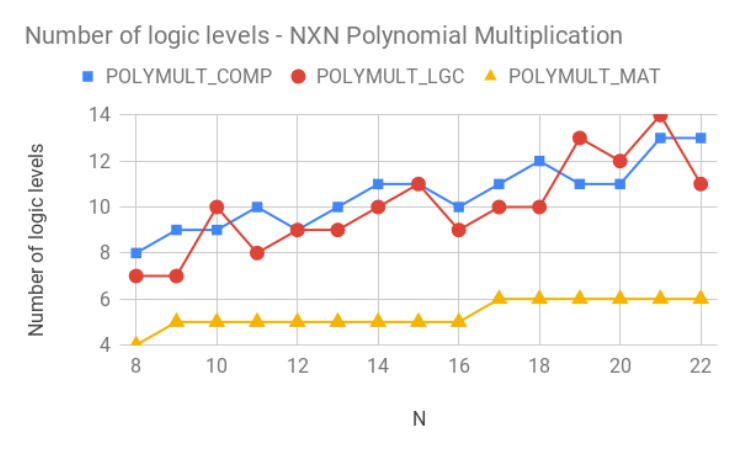
Delay on one input causes an extra toggle.

Bigger cells in SBox LGC to meet timing - Each toggle of LGC SBox is more expensive.

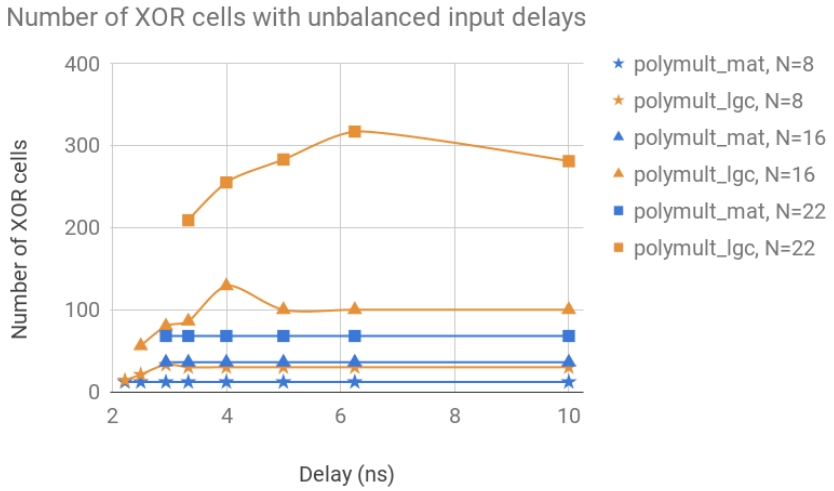
Impact of Logic Synthesis

Benchmark 2 : Binary Polynomial Multiplier

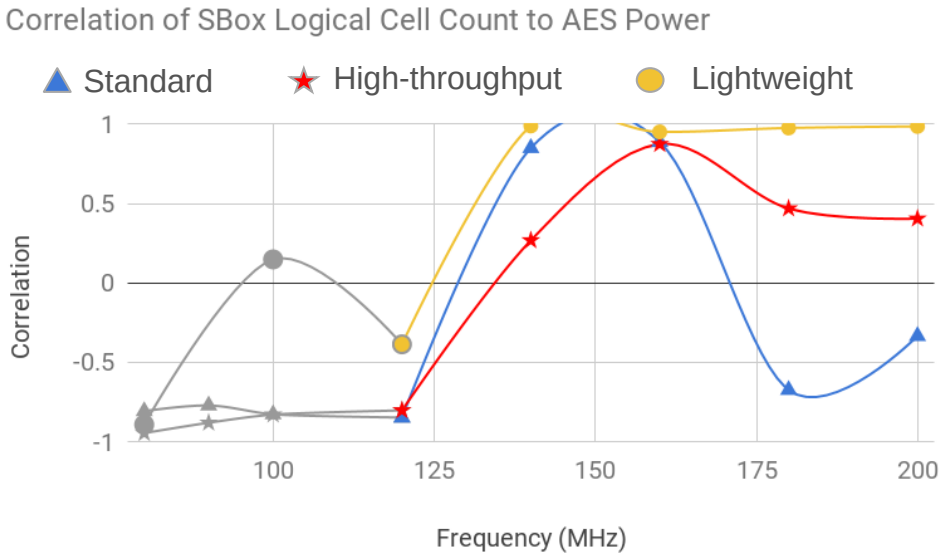
Technology-independent Comparison



Gates with unbalanced input delays



Post-synthesis Power of AES designs

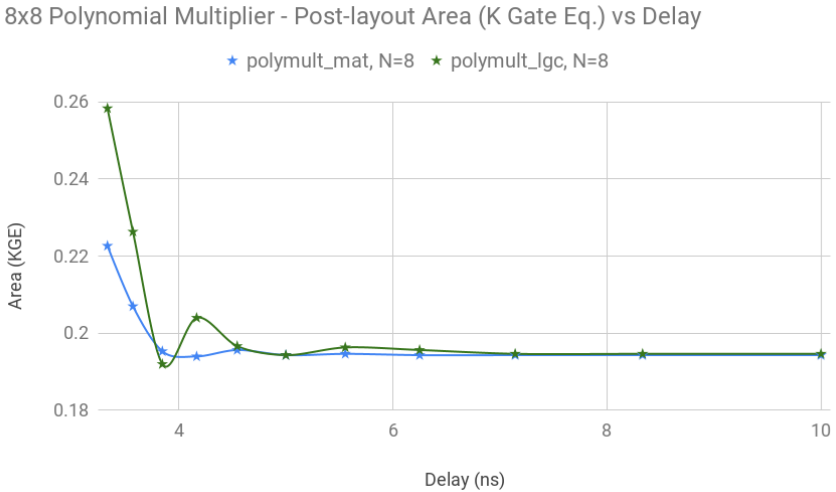


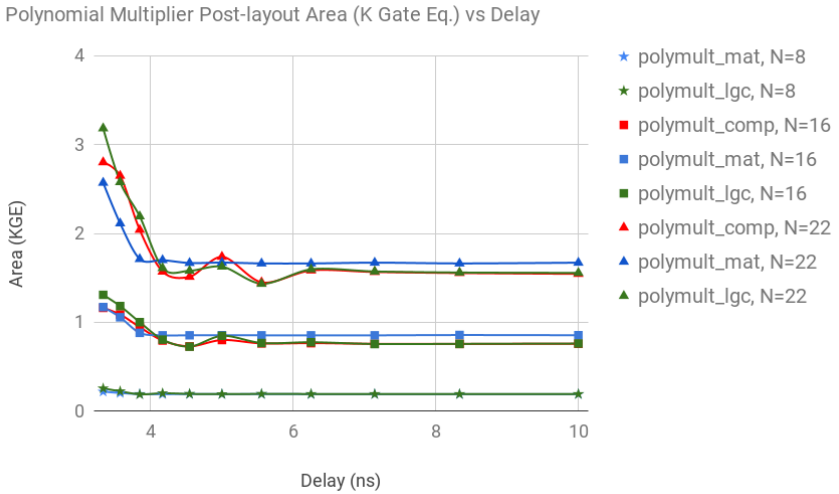
Region	AES Type	LGC *vs* LUT	LGC *vs* Canright
Minimal-Area	Standard	12-25% higher	12-21% lower
	High-Throughput	30-40% higher	15% lower
	Lightweight	20-25% higher	12-18% lower
High-Speed	Standard	5-20% lower	5-10% lower
	High-Throughput	5-15% lower	5% lower
	Lightweight	30% lower	~10% lower

Low correlation of gate count to power - toggling properties not well-captured by logical metrics.

Post-Layout results

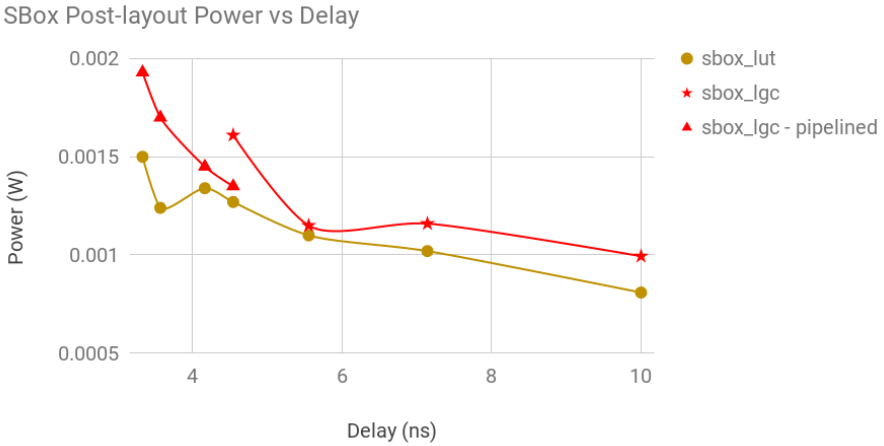
Polynomial Multiplier - Area



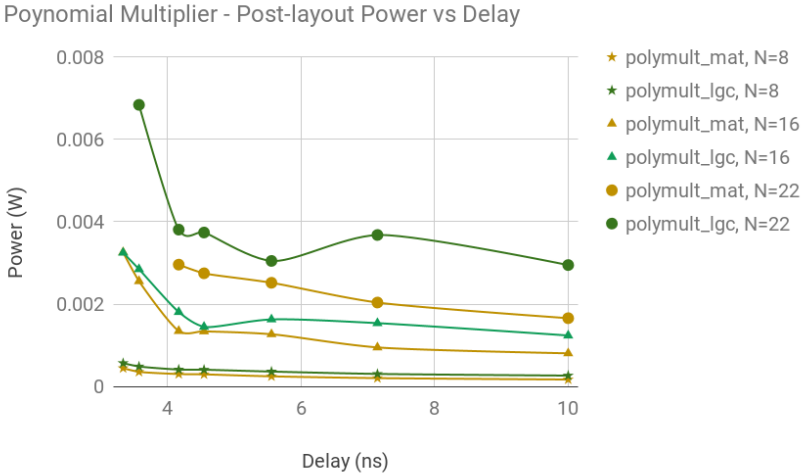


Post-Layout results

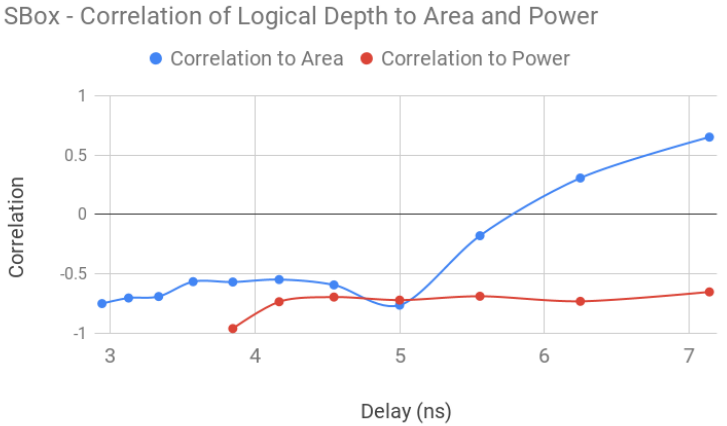
SBox - Power

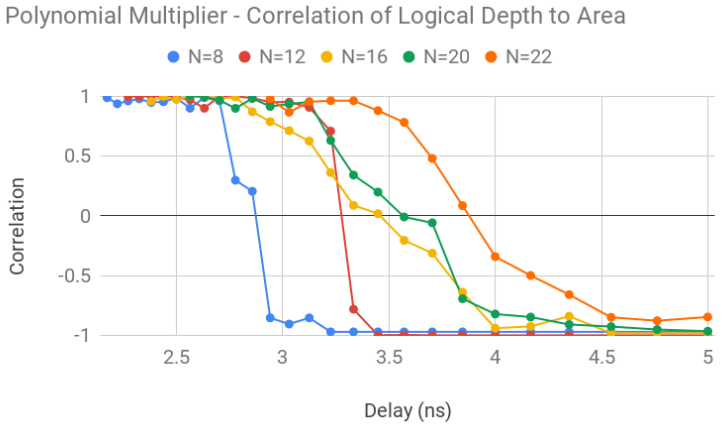


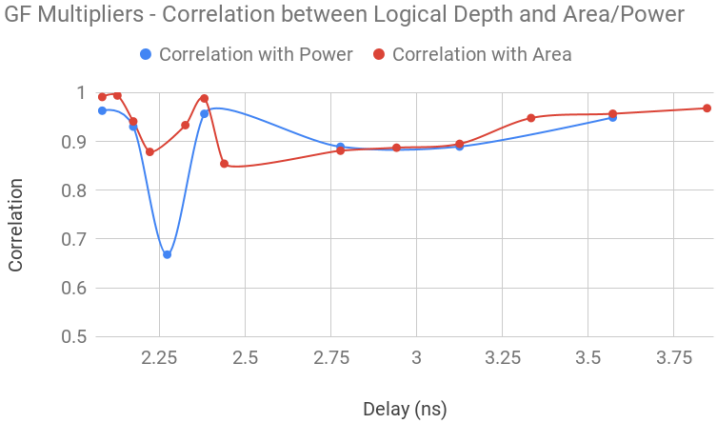
Polynomial Multiplier- Power

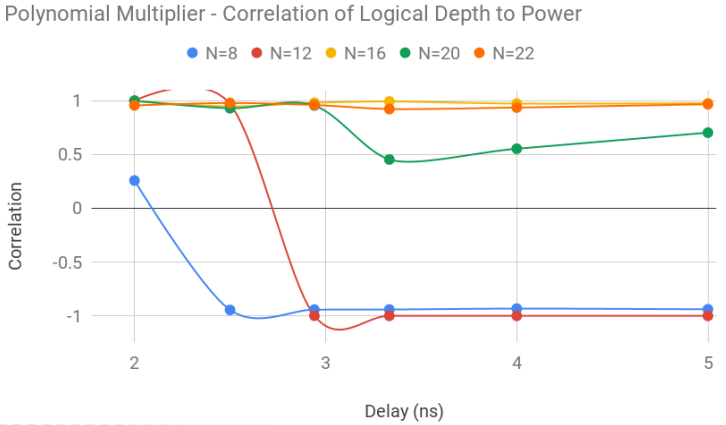


Correlation of logical depth to hardware metrics









Lightweight AES Designs - Area and Power