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

- Circuits expressed as AND/XOR/NOT logic operations.
- Closer estimate of hardware as compared to abstract input-output relationship.
- Easy to factor out redundant sub-expressions.

T1 = A ^ B
T2 = B & C
T3 = T1 & T2
T4 = T3 ^~ D
S = T2 & T4
Expectation
Fewer logic gates
Smaller hardware

Gate count used to compare crypto designs

Low Gate Count (LGC) circuits

Specialized Tools to minimize gate count

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

scheme using a smaller number of AND and XOR gates than in known schemes, although maintaining a comparable time delay. For example, in Table 3 we have summarized the resulting

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
Efficiency of Logic Minimization Techniques for Cryptographic 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).

![Logical gate count of SBox designs](chart)

![Logical Depth of SBox designs](chart)
Post-synthesis Area of SBox designs

- 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.

### LUT and LGC SBoxes - Area (K Gate Eq.) vs Delay

- Area of LGC designs blows up sooner
- LUT design reaches higher speeds

### LGC vs LUT

<table>
<thead>
<tr>
<th></th>
<th>Minimal-Area</th>
<th>High-Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>LGC vs LUT</td>
<td>50% smaller</td>
<td>40% larger</td>
</tr>
<tr>
<td>LGC vs Canright</td>
<td>20% smaller</td>
<td>25% larger</td>
</tr>
</tbody>
</table>

### Area of common Standard cells - 180 nm technology

- Drive Strength - X1
- Drive Strength - X2
- Drive Strength - X4

**Graphs and Data:**
- Area vs Delay
- Comparison of LUT vs LGC vs Canright
- Graph showing area of standard cells with drive strengths.
Post-synthesis Area of SBox designs

LUT and LGC SBoxes - Area (K Gate Eq.) vs Delay

- sbox_lut
- sbox_lgc
- sbox_canright
- sbox_lgc - Pipelined
- sbox_canright - Pipelined

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

Inserting a pipeline stage

Pipelining arrests area blow-up
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

<table>
<thead>
<tr>
<th></th>
<th>LGC vs LUT</th>
<th>LGC vs Canright</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimal-Area</td>
<td>50% smaller</td>
<td>20% smaller</td>
</tr>
<tr>
<td>High-Speed</td>
<td>40% larger</td>
<td>25% larger</td>
</tr>
<tr>
<td>High-Speed (with pipeline)</td>
<td>± 15%</td>
<td>10-15% larger</td>
</tr>
</tbody>
</table>
Post-synthesis Power of SBox designs

<table>
<thead>
<tr>
<th></th>
<th>LGC vs LUT</th>
<th>LGC vs Canright</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimal-Area</strong></td>
<td>15-20% lower</td>
<td>30% lower</td>
</tr>
<tr>
<td><strong>High-Speed</strong></td>
<td>30-45% higher</td>
<td>15-20% higher</td>
</tr>
<tr>
<td><strong>High-Speed</strong> (with pipeline)</td>
<td>20-30% higher</td>
<td>10-20% higher</td>
</tr>
</tbody>
</table>

- 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 $N$.

![Graph showing area vs delay for SBox after synthesis and place&route]

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

<table>
<thead>
<tr>
<th>Region</th>
<th>AES Type</th>
<th>LGC vs LUT</th>
<th>LGC vs Canright</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimal-Area</strong></td>
<td>Standard</td>
<td>12-32% smaller</td>
<td>7-13% smaller</td>
</tr>
<tr>
<td></td>
<td>High-Speed</td>
<td>18-33% smaller</td>
<td>5-13% smaller</td>
</tr>
<tr>
<td></td>
<td>Lightweight</td>
<td>8% smaller</td>
<td>4-8% smaller</td>
</tr>
<tr>
<td><strong>High-Speed</strong></td>
<td>Standard</td>
<td>9-16% smaller</td>
<td>6-14% smaller</td>
</tr>
<tr>
<td></td>
<td>High-Speed</td>
<td>11-19% smaller</td>
<td>1-7% smaller</td>
</tr>
<tr>
<td></td>
<td>Lightweight</td>
<td>9% smaller</td>
<td>± 5%</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Logical Metric</th>
<th>Design</th>
<th>Min-area Region</th>
<th>High-Speed Region</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Area</td>
<td>Power</td>
</tr>
<tr>
<td>Gate Count</td>
<td>SBox</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>Polynomial Multiplier</td>
<td>N ≤ 14</td>
<td>H</td>
</tr>
<tr>
<td></td>
<td></td>
<td>N &gt; 14</td>
<td>H</td>
</tr>
<tr>
<td></td>
<td>GF Multiplier</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>GF Inverter</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>AES Standard</td>
<td>H</td>
<td>L</td>
</tr>
<tr>
<td></td>
<td>High-throughput</td>
<td>H</td>
<td>L</td>
</tr>
<tr>
<td></td>
<td>Lightweight</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>Logical Depth</td>
<td>SBox</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td></td>
<td>Polynomial Multiplier</td>
<td>N ≤ 14</td>
<td>L</td>
</tr>
<tr>
<td></td>
<td></td>
<td>N &gt; 14</td>
<td>L</td>
</tr>
<tr>
<td></td>
<td>GF Multiplier</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td></td>
<td>GF Inverter</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td></td>
<td>AES Standard</td>
<td>H</td>
<td>L</td>
</tr>
<tr>
<td></td>
<td>High-throughput</td>
<td>H</td>
<td>L</td>
</tr>
<tr>
<td></td>
<td>Lightweight</td>
<td>M</td>
<td>L</td>
</tr>
</tbody>
</table>

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.

Area-Performance trade-off - AES SBox

- Only Cell Sizing
- Cell 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.

  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**

Number of logic levels - NXN Polynomial Multiplication

- POLYMULT_COMP
- POLYMULT_LGC
- POLYMULT_MAT

Number of XOR cells with unbalanced input delays

- polymult_mat, N=8
- polymult_lgc, N=8
- polymult_mat, N=16
- polymult_lgc, N=16
- polymult_mat, N=22
- polymult_lgc, N=22
Post-synthesis Power of AES designs

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

<table>
<thead>
<tr>
<th>Region</th>
<th>AES Type</th>
<th>LGC vs LUT</th>
<th>LGC vs Canright</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimal-Area</td>
<td>Standard</td>
<td>12-25% higher</td>
<td>12-21% lower</td>
</tr>
<tr>
<td></td>
<td>High-Throughput</td>
<td>30-40% higher</td>
<td>15% lower</td>
</tr>
<tr>
<td></td>
<td>Lightweight</td>
<td>20-25% higher</td>
<td>12-18% lower</td>
</tr>
<tr>
<td>High-Speed</td>
<td>Standard</td>
<td>5-20% lower</td>
<td>5-10% lower</td>
</tr>
<tr>
<td></td>
<td>High-Throughput</td>
<td>5-15% lower</td>
<td>5% lower</td>
</tr>
<tr>
<td></td>
<td>Lightweight</td>
<td>30% lower</td>
<td>~10% lower</td>
</tr>
</tbody>
</table>
Post-Layout results

Polynomial Multiplier - Area

8x8 Polynomial Multiplier - Post-layout Area (K Gate Eq.) vs Delay

- $\text{polymult}\_\text{mat}, N=8$
- $\text{polymult}\_\text{lrc}, N=8$

Polynomial Multiplier Post-layout Area (K Gate Eq.) vs Delay

- $\text{polymult}\_\text{mat}, N=8$
- $\text{polymult}\_\text{lrc}, N=8$
- $\text{polymult}\_\text{comp}, N=16$
- $\text{polymult}\_\text{mat}, N=16$
- $\text{polymult}\_\text{lrc}, N=16$
- $\text{polymult}\_\text{comp}, N=22$
- $\text{polymult}\_\text{mat}, N=22$
- $\text{polymult}\_\text{lrc}, N=22$
Post-Layout results

SBox - Power

![SBox Post-layout Power vs Delay](image)

Polynomial Multiplier - Power

![Polynomial Multiplier - Post-layout Power vs Delay](image)
Correlation of logical depth to hardware metrics

SBox - Correlation of Logical Depth to Area and Power
- Blue dots: Correlation to Area
- Red dots: Correlation to Power

GF Multipliers - Correlation between Logical Depth and Area/Power
- Blue dots: Correlation with Power
- Red dots: Correlation with Area

Polynomial Multiplier - Correlation of Logical Depth to Area
- N=8
- N=12
- N=16
- N=20
- N=22

Polynomial Multiplier - Correlation of Logical Depth to Power
- N=8
- N=12
- N=16
- N=20
- N=22
Lightweight AES Designs - Area and Power

Lightweight AES - Area vs Throughput

Lightweight AES - Area vs Throughput

Throughput (M Encryptions per sec)

Throughput (M Encryptions per sec)