Spin Me Right Round: Rotational Symmetry for FPGA-Specific AES

CHES 2018, Amsterdam

Lauren De Meyer\textsuperscript{1}, Amir Moradi\textsuperscript{2}, Felix Wegener\textsuperscript{2}

\textsuperscript{1} imec - COSIC, KU Leuven, Belgium
\textsuperscript{2} Horst Görtz Institute for IT-Security, Ruhr-Universität Bochum, Germany
Area Optimization: ASICs vs FPGAs

ASIC

[Diagram of logic gates]
Area Optimization: ASICs vs FPGAs

ASIC

FPGA (Xilinx 6/7 series)

Spartan-6 FPGA Configurable Logic Block User Guide
FPGA Building Blocks (Xilinx)

- **Slice contents:**
  - 4 LUT6 elements
  - Auxiliar MUX
  - (8 registers)
FPGA Building Blocks (Xilinx)

- Slice contents:
  - 4 LUT6 elements
  - Auxiliar MUX
  - (8 registers)

One slice can implement any $\mathbb{F}_2^8 \rightarrow \mathbb{F}_2$ function
AES S-box Structure

\[ x^{-1} = x^{254} \quad \text{in} \quad GF(2^8) \]

Power Map

Affine Map

\[ Ax + b \]
AES S-box in FPGAs

- Naive Approach: one slice per coordinate: 8 slices
AES S-box in FPGAs

- Naive Approach: one slice per coordinate: 8 slices

- Algebraic degree 7 $\rightarrow$ no obvious improvements
AES S-box in FPGAs

- **Naive Approach:** one slice per coordinate: **8 slices**

- Algebraic degree 7 $\rightarrow$ no obvious improvements
- Tower field doesn’t suit LUTs

Canright. *A Very Compact S-box for AES.* CHES 2005
AES S-box in FPGAs

- Naive Approach: one slice per coordinate: 8 slices

- Algebraic degree 7 → no obvious improvements

- Tower field doesn’t suit LUTs

Our Contribution: Reduction to 4 slices

Canright: A Very Compact S-box for AES. CHES 2005
Rotational Symmetry of Power Maps

Inversion in $GF(2^8)$: $x \mapsto x^{254}$

Conversion to normal base: $x \mapsto \phi(x)$

Rotation: $rot((a_0, \ldots, a_{n-1})) = (a_{n-1}, a_0, \ldots, a_{n-2})$
Rotational Symmetry of Power Maps

Inversion in $GF(2^8)$: $x \mapsto x^{254}$

Conversion to normal base: $x \mapsto \phi(x)$

Rotation: $\text{rot}( (a_0, \ldots, a_{n-1}) ) = (a_{n-1}, a_0, \ldots, a_{n-2})$

Theorem$^1$:

Power Map: $F(x) = x^m$ in $GF(2^8)$

Normal base: $S(x) = \phi(F(\phi^{-1}(x)))$

$\Rightarrow$

$\text{rot}(S(x)) = S(\text{rot}(x))$

$^1$ Rijmen, Barreto, Gazzoni Filho. Rotation Symmetry in Algebraically Generated Cryptographic Substitution Tables. Information Processing Letters 2008
Rotational Symmetry: Area Reduction

Idea: Create circuit for **only one** coordinate function (LSB)

LSB of S-box: $S^*$
Rotational Symmetry: Area Reduction

Idea: Create circuit for **only one** coordinate function (LSB)

LSB of S-box: S*
Rotational Symmetry: Area Reduction

Idea: Create circuit for **only one** coordinate function (LSB)
Rotational Symmetry: Area Reduction

Idea: Create circuit for **only one** coordinate function (LSB)
AES S-box: Byte-serial Circuit

- Transformation to (p2n) and from (n2p) normal basis
- Occupies 4 slices: 16LUTs / 15Regs
- Latency: 8 cycles
First Design:
Improve smallest FPGA-specific AES
Former record by Sasdrich et al.\textsuperscript{1}

- **21 slices** on Xilinx Spartan-6
- **15 slices shown + 6 for control unit**

\textsuperscript{1}Sasdrich, Güneysu. *A grain in the silicon: SCA-protected AES in less than 30 slices*. ASAP 2016
Former record by Sasdrich et al.\textsuperscript{1}

- **21 slices** on Xilinx Spartan-6
- **15 slices** shown + 6 for control unit

\textsuperscript{1}Sasdrich, Güneysu. *A grain in the silicon: SCA-protected AES in less than 30 slices*. ASAP 2016
Former record by Sasdrich et al.\(^1\)

- **21 slices** on Xilinx Spartan-6
- **15 slices shown + 6 for control unit**

Total design: 17 slices

---

\(^1\) Sasdrich, Güneysu. *A grain in the silicon: SCA-protected AES in less than 30 slices.* ASAP 2016
Second Design:
Port smallest AES on ASICs to FPGAs
Bitsliding Design: Jean et al, CHES 2017

Adapt smallest ASIC-based AES to FPGAs

Jean, Moradi, Peyrin, Sasdrich. *Bit-sliding: A generic technique for bit-serial implementations of SPN-based primitives - applications to AES, PRESENT and SKINNY.* CHES 2017
Bitsliding Design: Jean et al, CHES 2017

Adapt smallest ASIC-based AES to FPGAs

Jean, Moradi, Peyrin, Sasdrich. *Bit-sliding: A generic technique for bit-serial implementations of SPN-based primitives - applications to AES, PRESENT and SKINNY.* CHES 2017
Fully-bitserial S-box

- Bitserial in-/output
- Area: 4 slices: 16 LUTs, 16 Regs
- Latency: 16 Cycles
Bitsliding Design: Jean et al, CHES 2017

Adapt smallest ASIC-based AES to FPGAs

Jean, Moradi, Peyrin, Sasdrich. *Bit-sliding: A generic technique for bit-serial implementations of SPN-based primitives - applications to AES, PRESENT and SKINNY.* CHES 2017
Bitsliding on an FPGA

- 4 LUTs as 32-bit shift registers
- Shiftrows: 32 cycles
- Mixcolumns: 32 cycles

Total design: 63 LUTs
## Comparison

<table>
<thead>
<tr>
<th>Design</th>
<th># LUTs</th>
<th># Flipflops</th>
<th># Slices</th>
<th>#Clockcyc.</th>
<th>Max. Freq.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sasdrich et al. [SG16]</td>
<td>84</td>
<td>24</td>
<td>21</td>
<td>1471</td>
<td>108 Mhz</td>
</tr>
<tr>
<td>Our AES based on [SG16]</td>
<td>68</td>
<td>39</td>
<td>17</td>
<td>5538</td>
<td>109 Mhz</td>
</tr>
<tr>
<td>Our AES based on [JMPS17]</td>
<td>63</td>
<td>38</td>
<td>19</td>
<td>4852</td>
<td>155 Mhz</td>
</tr>
</tbody>
</table>

Third Design:
Smallest First-order secure AES on FPGAs
Masking

- Decomposition into cubic function\(^1\):
  \[ x^{-1} = x^{254} = (x^{26})^{49} \]

- Implement **one** coordinate of each cubic function:
  \[ G^*(\phi(x)) = \phi(x^{26}), \quad F^*(\phi(x)) = \phi(x^{49}) \]

\(^1\) Moradi. *Advances in Side-channel Security*. 2016
Masking

- Decomposition into cubic function\(^1\):
  \[ x^{-1} = x^{254} = (x^{26})^{49} \]

- Implement **one** coordinate of each cubic function:
  \[ G^*(\phi(x)) = \phi(x^{26}), \quad F^*(\phi(x)) = \phi(x^{49}) \]

- Find first-order masking (CMS\(^2\)):
  any-order: \( d + 1 \) input sh. / \( (d + 1)^t \) output sh.
  first-order: 2 input shares / 8 output shares

---

\(^1\) Moradi. *Advances in Side-channel Security*. 2016
Masking

- Decomposition into cubic function\(^1\):
  \[ x^{-1} = x^{254} = (x^{26})^{49} \]

- Implement **one** coordinate of each cubic function:
  \[ G^*(\phi(x)) = \phi(x^{26}), \quad F^*(\phi(x)) = \phi(x^{49}) \]

- Find first-order masking (CMS\(^2\)):
  
  **any-order:** \( d + 1 \) input sh. / \((d + 1)^t\) output sh.  
  **first-order:** 2 input shares / 8 output shares

**Problem:** How to find CMS sharing of cubic function?

---

\(^1\) Moradi. *Advances in Side-channel Security*. 2016  
Masking

- Decomposition into cubic function\(^1\):
  \[ \begin{align*}
  x - 1 &= x^254 = x^2649 \\
  \end{align*} \]

- Implement one coordinate of each cubic function:
  \[ \begin{align*}
  G \ast \phi(x) &= \phi(x^{26}) \\
  F \ast \phi(x) &= \phi(x^{49}) \\
  \end{align*} \]

- Find first-order masking (CMS\(^2\)):
  \[ \begin{align*}
  \text{any-order: } d \text{ input shares} / d + 1 \text{ output shares} \\
  \text{first-order: } 2 \text{ input shares} / 8 \text{ output shares} \\
  \end{align*} \]

**Solution: Our Heuristic**

Split function \( G \) into parts: \( G^A, G^B, G^C \)

2 input shares / 8 output shares each

(Details in the paper)

---

\(^1\) Moradi. *Advances in Side-channel Security*. 2016

Non-complete realization of F*/G*

- 18 bits of randomness / cycle
- Dependence on only 14 bits each reduces area

Data flow:

- $r_0 \rightarrow G^A$
- $r_1 \rightarrow G^B$
- $r_2 \rightarrow G^C$
- $r_3 \rightarrow (F \oplus G)^A$
- $r_4 \rightarrow (F \oplus G)^B$
- $r_5 \rightarrow (F \oplus G)^C$

Size: 144 LUTs, 48 Regs
Two-share S-box

- First-order secure design
- Clear register to $F^*/G^*$ on negative edge
- Area: 182 LUTs, 96 Reg
- Latency: 26 cycles
SCA Evaluation: Moments-Correlating DPA

Measurement Setup:

- Sakura-G platform
- Oscilloscope: 625 MS/s
- Target: 6 MHz
- Additional AC amplifier

![Graph showing correlation over time with PRNG off, 1st order, 10k traces]
SCA Evaluation: Moments-Correlating DPA

Measurement Setup:

- Sakura-G platform
- Oscilloscope: 625 MS/s
- Target: 6 MHz
- Additional AC amplifier

![Graphs showing correlation over time for PRNG off, 1st order with 10k traces and PRNG on, 1st order with 10M traces.](image)

![Graphs showing correlation over time for PRNG on, 2nd order with 10k traces.](image)
## Comparison: First-order secure Designs

<table>
<thead>
<tr>
<th>Design</th>
<th># LUTs</th>
<th># FF</th>
<th># Slices</th>
<th>#Cycles</th>
<th>#Rand. Bits</th>
<th>Max. Freq.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bilgin et al. [BGN+15]</td>
<td>1198</td>
<td>611</td>
<td>475</td>
<td>246</td>
<td>32</td>
<td>127 MHz</td>
</tr>
<tr>
<td>Gross et al [GMK17]</td>
<td>595</td>
<td>734</td>
<td>366</td>
<td>246</td>
<td>18</td>
<td>103 MHz</td>
</tr>
<tr>
<td>Cnudde et al [CRB+16]</td>
<td>1191</td>
<td>642</td>
<td>553</td>
<td>275</td>
<td>54</td>
<td>181 MHz</td>
</tr>
<tr>
<td>This work</td>
<td>293</td>
<td>124</td>
<td>162</td>
<td>6852</td>
<td>18</td>
<td>103 MHz</td>
</tr>
</tbody>
</table>


Summary

This presentation:
- New size-record for FPGA-specific AES
- Smallest first-order secure AES on FPGA devices

Further contributions in the paper:
- Latency optimizations for the Sasdrich et al. design
- New heuristic to mask Boolean functions with $d + 1$ Shares
Thanks!
any questions?

felix.wegener@rub.de

Lauren De Meyer\textsuperscript{1}, Amir Moradi\textsuperscript{2}, Felix Wegener\textsuperscript{2}

\textsuperscript{1} imec - COSIC, KU Leuven, Belgium
\textsuperscript{2} Horst Görtz Institute for IT-Security, Ruhr-Universität Bochum, Germany