A Lightweight AES Implementation Against Bivariate First-Order DPA Attacks

Weize Yu and Selçuk Köse

Department of Electrical Engineering
University of South Florida
Side-channel attacks

Power analysis attacks (PAA)

Previous countermeasures against PAA

Aggressive voltage scaling (AVS) against conventional first-order (CFO) DPA attacks

Bivariate first-order (BFO) DPA attacks on cryptographic circuit with AVS technique

Proposed countermeasure for securing cryptographic circuit with AVS technique against BFO DPA attacks

Conclusion
Why Hardware Security is Important?
Side-Channel Attacks

Possible side-channel attacks

- Power Consumption
- EM Emissions
- Faulty Outputs
- Design Details
- Output
- Input
- Timing
- Sound
- Heat
Presentation Flow

- Side-channel attacks
- Power analysis attacks (PAA)
- Previous countermeasures against PAA
- Aggressive voltage scaling (AVS) against conventional first-order (CFO) DPA attacks
- Bivariate first-order (BFO) DPA attacks on cryptographic circuit with AVS technique
- Proposed countermeasure for securing cryptographic circuit with AVS technique against BFO DPA attacks
- Conclusion
Power Analysis Attacks

Chip without protection

Power supply

Input data

Core

Cryptographic circuit

Cipher data

Cryptographic chip

Key inside
Simple Power Analysis (SPA) Attacks

Simple Power Analysis: Directly analyze (few) traces, for example RSA:
Conventional First-Order (CFO) Differential Power Analysis (DPA) Attacks

Results of CFO DPA Attacks

Successful CFO DPA attacks

Unsuccessful CFO DPA attacks

Correlation coefficient between the correct key and monitored power consumption is important

Presentation Flow

- Side-channel attacks
- Power analysis attacks (PAA)
- Previous countermeasures against PAA
- Aggressive voltage scaling (AVS) against conventional first-order (CFO) DPA attacks
- Bivariate first-order (BFO) DPA attacks on cryptographic circuit with AVS technique
- Proposed countermeasure for securing cryptographic circuit with AVS technique against BFO DPA attacks
- Conclusion
Power information leakage

0-1 and 1-0 are the same
0-0 and 1-1 are the same

Combine them together

Power Supply Scrambling


### Staggered switching pattern

<table>
<thead>
<tr>
<th>SC Module</th>
<th>Sequence</th>
<th>$t_0$</th>
<th>$t_1$</th>
<th>$t_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>S1</td>
<td>Red</td>
<td>Blue</td>
<td>Purple</td>
</tr>
<tr>
<td></td>
<td>S2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>S3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>S1</td>
<td>Purple</td>
<td>Red</td>
<td>Blue</td>
</tr>
<tr>
<td></td>
<td>S2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>S3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>S1</td>
<td>Blue</td>
<td>Purple</td>
<td>Red</td>
</tr>
<tr>
<td></td>
<td>S2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>S3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3 switching states: S1, S2, S3

- **S1**: Charge the capacitor from the supply
- **S2**: Provide charge to the core for encryption
- **S3**: Discharge the capacitor to a pre-defined value

**Drawback**: High power/area/performance overhead
Power Delivery Network (PDN) Modification

Drawback: High PDN impedance hurts the circuit's energy efficiency and robustness

Random Dynamic Voltage Scaling (RDVS)


Drawback: High power overhead

\[ P_{\text{dyn}} = \alpha CV_{dd}^2 f_c \]

Input data dependent

Randomly alter \( V_{dd} \)
Plaintexts Masking

Add random mask

Masked Algorithm

Remove random mask

Ciphertext

Random Mask

Mask Modification

Drawback: High area/performance overhead due to a large amount of mask data

Side-channel attacks
Power analysis attacks (PAA)
Previous countermeasures against PAA
Aggressive voltage scaling (AVS) against conventional first-order (CFO) DPA attacks
Bivariate first-order (BFO) DPA attacks on cryptographic circuit with AVS technique
Proposed countermeasure for securing cryptographic circuit with AVS technique against BFO DPA attacks
Conclusion
Aggressive Voltage Scaling (AVS) Technique


<table>
<thead>
<tr>
<th>Scheme</th>
<th>Area</th>
<th>Power</th>
<th>Performance</th>
<th>PVT Tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logic Style (WDDL)</td>
<td>3X</td>
<td>4X</td>
<td>.25X</td>
<td>×</td>
</tr>
<tr>
<td>Masking</td>
<td>3X</td>
<td>-</td>
<td>0.5X</td>
<td>×</td>
</tr>
<tr>
<td>RDVFS</td>
<td>-</td>
<td>0.73X</td>
<td>0.85X</td>
<td>×</td>
</tr>
<tr>
<td>AFS</td>
<td>1.03X</td>
<td>1.05X</td>
<td>1.57X</td>
<td>√</td>
</tr>
<tr>
<td>AVS</td>
<td>1.03X</td>
<td>0.5X</td>
<td>0.95X</td>
<td>√</td>
</tr>
</tbody>
</table>

Low overhead

AVS technique
Effective countermeasures against DPA attacks on S-boxes using AVS technique.

Successful DPA attacks on an S-box without countermeasure after inputting 10 thousand plaintexts.

Unsuccessful DPA attacks on an S-box with AVS technique after inputting 1 million plaintexts.

Side-channel attacks

Power analysis attacks (PAA)

Previous countermeasures against PAA

Aggressive voltage scaling (AVS) against conventional first-order (CFO) DPA attacks

Bivariate first-order (BFO) DPA attacks on cryptographic circuit with AVS technique

Proposed countermeasure for securing cryptographic circuit with AVS technique against BFO DPA attacks

Conclusion
BFO DPA Attacks on a Cryptographic Circuit with AVS Technique

Two adjacent power consumptions of a cryptographic circuit with AVS technique

\[ P_{dyn,j} = \beta_{0 \rightarrow 1,j} f_c V_{dd,[j]}^2 C_L \]
\[ P_{dyn,j+1} = \beta_{0 \rightarrow 1,j+1} f_c V_{dd,[j+1]}^2 C_L \]

\[ \frac{P_{dyn,j+1}}{P_{dyn,j}} = \frac{\beta_{0 \rightarrow 1,j+1}}{\beta_{0 \rightarrow 1,j}} \]

V_{dd} changes slowly

CFO DPA attacks

Two adjacent input data

X_j  
X_{j+1}

BFO DPA attacks

\[ X_{j+1}/X_j \]

The power noise induced by randomly reshuffling Supply voltage V_{dd} is eliminated by executing BFO DPA attacks!
Results of DPA Attacks on S-Boxes with AVS Technique

Successful CFO DPA attacks on an S-box without countermeasure after inputting 1 thousand plaintexts

Unsuccessful CFO DPA attacks on an S-box with AVS technique after inputting 100 thousand plaintexts

Successful BFO DPA attacks on an S-box with AVS technique after inputting 6 thousand plaintexts
Presentation Flow

Side-channel attacks
Power analysis attacks (PAA)
Previous countermeasures against PAA
Aggressive voltage scaling (AVS) against conventional first-order (CFO) DPA attacks
Bivariate first-order (BFO) DPA attacks on cryptographic circuit with AVS technique
Proposed countermeasure for securing cryptographic circuit with AVS technique against BFO DPA attacks
Conclusion
Advanced Encryption Standard (AES)
Cryptographic Algorithm

Plaintext

Add round key

Substitute bytes

Shift rows

Mix columns

Add round key

Round 1

Substitute bytes

Shift rows

Mix columns

Add round key

Round 2

Round m-1

Substitute bytes

Shift rows

Mix columns

Add round key

Round m

Ciphertext

DPA attacks
DPA Attacks on AES Engine

1st encryption round of a typical 128-bit AES engine

Select input plaintexts to simplify DPA attacks.
Proposed Lightweight Masked AES Engine

Conventional AES engine (1st encryption round)

Proposed lightweight masked AES engine (1st encryption round)

Mask: $m=(00000000), (11111111), (00000000), (11111111), \ldots$  Constant sequence

or $m=(00000000), (00000000), (11111111), (00000000), \ldots$  Random sequence
Results of BFO DPA Attacks on AES Engines with AVS Technique

Successful BFO DPA attacks on a conventional AES engine with AVS technique after inputting 6 thousand plaintexts

Successful BFO DPA attacks on a lightweight masked AES engine (constant masking sequence) with AVS technique after inputting 500 thousand plaintexts

Unsuccessful BFO DPA attacks on a lightweight masked AES engine (random masking sequence) with AVS technique after inputting 1 million plaintexts
Side-channel attacks

Power analysis attacks (PAA)

Previous countermeasures against PAA

Aggressive voltage scaling (AVS) against conventional first-order (CFO) DPA attacks

Bivariate first-order (BFO) DPA attacks on cryptographic circuit with AVS technique

Proposed countermeasure for securing cryptographic circuit with AVS technique against BFO DPA attacks

Conclusion
Conclusion

- Cryptographic circuit is vulnerable against power analysis attacks

- Aggressive voltage scaling (AVS) technique is an efficient countermeasure against conventional first-order (CFO) DPA attacks with low overhead

- Conventional AES engine employs AVS technique is vulnerable against bivariate first-order (BFO) DPA attacks

- Lightweight random masked AES engine with AVS technique thwarts DPA attacks efficiently with negligible power/area/performance overhead
Thanks!