THRESHOLD IMPLEMENTATIONS OF ALL 3x3 AND 4x4 S-BOXES

B.Bilgin, S.Nikova, V.Nikov, V.Rijmen, G.Stütz

KU Leuven, UTwente, NXP, TU Graz

CHES 2012 - Leuven, Belgium
2012-09-10

KATHOLIEKE UNIVERSITEIT LEUVEN

Countermeasures

Search for a countermeasure against DPA

Countermeasures

Search for a countermeasure against DPA

- Hardware countermeasures
  - Balancing power consumption [Tiri et al., CHES'03]
  - ...
- Masking
  - Masking intermediate values [Chari et al., CRYPTO'99; Goubin et al., CHES'99]
  - Threshold Implementations [Nikova et al., ICISC'08]
  - Shamir's Secret Sharing [Goubin et al., CHES'11; Prouff et al., CHES'11]
  - ...

Countermeasures

Search for a countermeasure against DPA

- Hardware countermeasures
  - Balancing power consumption [Tiri et al., CHES'03]
  - ...
- Masking
  - Masking intermediate values [Chari et al., CRYPTO'99; Goubin et al., CHES'99]
  - Threshold Implementations [Nikova et al., ICISC'08]
  - Shamir's Secret Sharing [Goubin et al., CHES'11; Prouff et al., CHES'11]
  - ...

Issues: Unfeasible circuit size , glitches

Glitches

Temporary states of the output

Glitches

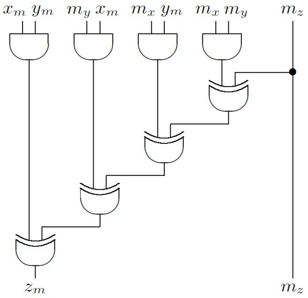
Temporary states of the output

$$z \quad = \quad x \; AND \; y \text{ , where } x_m = x \oplus m_x, y_m = y \oplus m_y$$

Glitches

Temporary states of the output

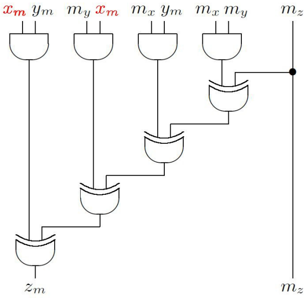
$$z = x\ AND\ y \text{ , where } x_m = x \oplus m_x, y_m = y \oplus m_y$$
$$z_m = x_m y_m \oplus (m_y x_m \oplus (m_x y_m \oplus (m_x m_y \oplus m_z)))$$



Glitches

Temporary states of the output

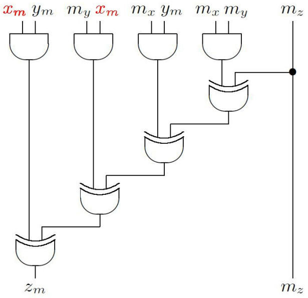
$$z = x\ AND\ y \text{ , where } x_m = x \oplus m_x, y_m = y \oplus m_y$$
$$z_m = x_m y_m \oplus (m_y x_m \oplus (m_x y_m \oplus (m_x m_y \oplus m_z)))$$



Glitches

Temporary states of the output

$$z = x\ AND\ y \text{ , where } x_m = x \oplus m_x, y_m = y \oplus m_y$$
$$z_m = x_m y_m \oplus (m_y x_m \oplus (m_x y_m \oplus (m_x m_y \oplus m_z)))$$



y	m_y	y_m	AND	XOR
0	0	0	0	0
0	1	1	2	2
1	0	1	1	1
1	1	0	1	2

Threshold Implementations

Threshold Implementations

- Any hardware technology
- Realistic size
- Provably secure against 1st order DPA

Threshold Implementations

Threshold Implementations

- Any hardware technology
- Realistic size
- Provably secure against 1^{st} order DPA

So far,

- Noekeon [Nikova et al., ICISC'08]
- Present [Poschmann et al., J.Cryptology'11]
- AES [Moradi et al., Eurocrypt'11]

Threshold Implementations

In this paper,

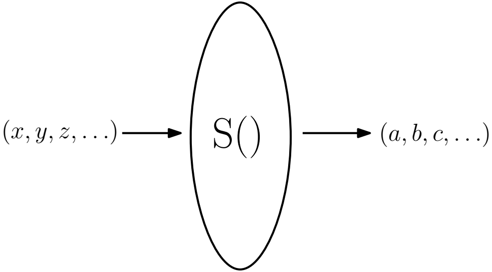
- TI of all 3×3 and 4×4 S-boxes
  - The non-linear part of a cipher
  - Common S-box size for lightweight crypto

Threshold Implementations

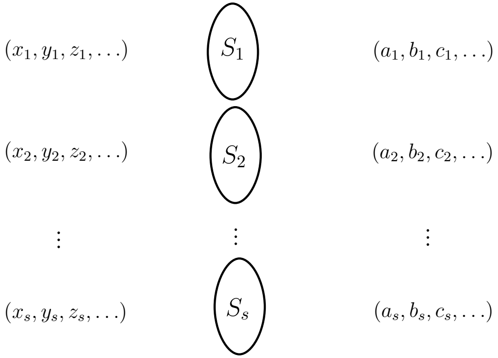
In this paper,

- TI of all 3×3 and 4×4 S-boxes
  - The non-linear part of a cipher
  - Common S-box size for lightweight crypto
- Cost of a TI

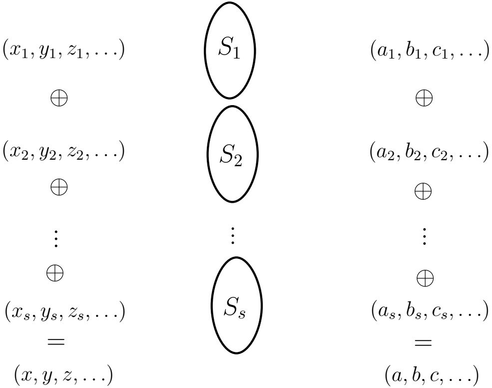
What is TI?



What is TI?

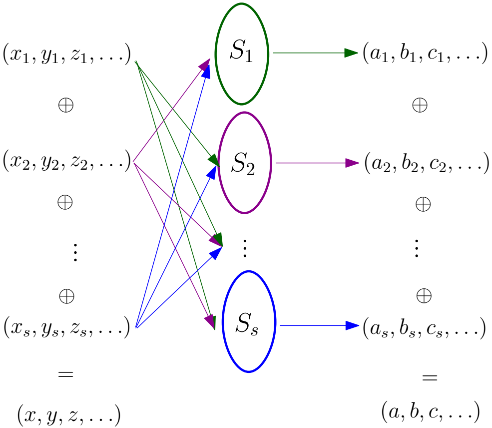

$(x_1, y_1, z_1, \ldots)$
S_1
$(a_1, b_1, c_1, \ldots)$
$(x_2, y_2, z_2, \ldots)$
S_2
$(a_2, b_2, c_2, \ldots)$
$(x_s, y_s, z_s, \ldots)$
S_s
$(a_s, b_s, c_s, \ldots)$

What is TI?



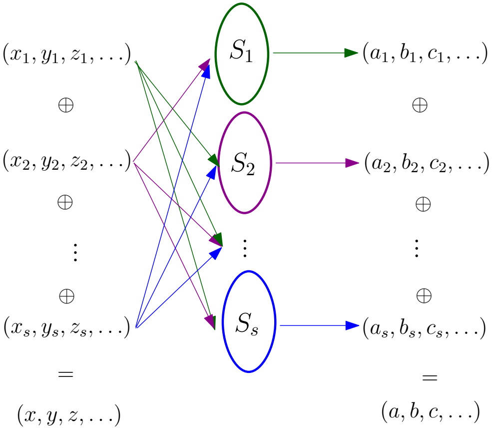
- Correct

What is TI?



- Correct
- Non-complete

What is TI?



- Correct
- Non-complete
- Uniform

Affine Equivalence Classes

Definition

$S_1(x)$ and $S_2(x)$ are affine equivalent if $\exists$ invertible affine permutations $A(x)$ and $B(x)$ s.t $S_1 = B \circ S_2 \circ A$

Affine Equivalence Classes

Theorem

If S_2 can be shared properly, then every S_1 that belongs to the same class with S_2 can be shared since $S_1 = B \circ S_2 \circ A$

Affine Equivalence Classes

Theorem

If S_2 can be shared properly, then every S_1 that belongs to the same class with S_2 can be shared since $S_1 = B \circ S_2 \circ A$

	3×3 S-boxes	4×4 S-boxes
Affine (A_i)	1	1
Quadratic (Q_i)	3	6
Cubic (C_i)	-	295

Affine Equivalence Classes

Theorem

If S_2 can be shared properly, then every S_1 that belongs to the same class with S_2 can be shared since $S_1 = B \circ S_2 \circ A$

	3×3 S-boxes	4×4 S-boxes
Affine (A_i)	1	1
Quadratic (Q_i)	3	6
Cubic (C_i)	-	295

Reduce the workspace

Affine Equivalence Classes

Theorem

If S_2 can be shared properly, then every S_1 that belongs to the same class with S_2 can be shared since $S_1 = B \circ S_2 \circ A$

	3×3 S-boxes	4×4 S-boxes
Affine (A_i)	1	1
Quadratic (Q_i)	3	6
Cubic (C_i)	-	295

Reduce the workspace

A function with degree d can be shared with at least $d + 1$ shares

Direct Sharing

$$
\begin{aligned}
S(x,y,z) &= x + yz \\
S_1 &= x_2 + y_2 z_2 + y_2 z_3 + y_3 z_2 \\
S_2 &= x_3 + y_3 z_3 + y_3 z_1 + y_1 z_3 \\
S_3 &= x_1 + y_1 z_1 + y_1 z_2 + y_2 z_1
\end{aligned}
$$

Direct Sharing

$$
\begin{aligned}
S(x, y, z) &= x + yz \\
S_1 &= x_2 + y_2z_2 + y_2z_3 + y_3z_2 \\
S_2 &= x_3 + y_3z_3 + y_3z_1 + y_1z_3 \\
S_3 &= x_1 + y_1z_1 + y_1z_2 + y_2z_1
\end{aligned}
$$

	3×3 S-boxes	4×4 S-boxes
Affine	A_0	A_0
Quadratic	Q_1, Q_2, Q_3	Q_4, Q_{12}, Q_{293}, Q_{294}, Q_{299}, Q_{300}

Correction Terms

$$
\begin{aligned}
S(x,y,z) &= x + yz \\
S_1 &= \cancel{x_2} + y_2 z_2 + y_2 z_3 + y_3 z_2 + \cancel{x_2} + x_3 \\
S_2 &= \cancel{x_3} + y_3 z_3 + y_3 z_1 + y_1 z_3 + \cancel{x_3} + x_1 \\
S_3 &= \cancel{x_1} + y_1 z_1 + y_1 z_2 + y_2 z_1 + \cancel{x_1} + x_2
\end{aligned}
$$

	3×3 S-boxes	4×4 S-boxes
Affine	A_0	A_0
Quadratic	Q_1, Q_2, Q_3	Q_4, Q_{12}, Q_{293}, Q_{294}, Q_{299}, Q_{300}

Correction Terms

$$
\begin{aligned}
S(x,y,z) &= x + yz \\
S_1 &= \cancel{x_2} + y_2z_2 + y_2z_3 + y_3z_2 + \cancel{x_2} + x_3 \\
S_2 &= \cancel{x_3} + y_3z_3 + y_3z_1 + y_1z_3 + \cancel{x_3} + x_1 \\
S_3 &= \cancel{x_1} + y_1z_1 + y_1z_2 + y_2z_1 + \cancel{x_1} + x_2
\end{aligned}
$$

	3×3 S-boxes	4×4 S-boxes
Affine	A_0	A_0
Quadratic	Q_1, Q_2, Q_3	Q_4, Q_{12}, Q_{293}, Q_{294}, Q_{299}, Q_{300}

Work for n shares with m variables is $2^{3(m+\binom{m}{2})n}$

3x3 S-box with 3 shares $2^{18\times 3} = 2^{54}$

Correction Terms

$$
\begin{aligned}
S(x,y,z) &= x + yz \\
S_1 &= \cancel{x_2} + y_2 z_2 + y_2 z_3 + y_3 z_2 + \cancel{x_2} + x_3 \\
S_2 &= \cancel{x_3} + y_3 z_3 + y_3 z_1 + y_1 z_3 + \cancel{x_3} + x_1 \\
S_3 &= \cancel{x_1} + y_1 z_1 + y_1 z_2 + y_2 z_1 + \cancel{x_1} + x_2
\end{aligned}
$$

	3×3 S-boxes	4×4 S-boxes
Affine	A_0	A_0
Quadratic	Q_1, Q_2, Q_3	Q_4, Q_{12}, Q_{293}, Q_{294}, Q_{299}, Q_{300}

Work for n shares with m variables is $2^{3(m+\binom{m}{2})n}$

3x3 S-box with 3 shares $2^{18 \times 3} = 2^{54}$

How to share Q_3 or Q_{300} in one step

Decomposition

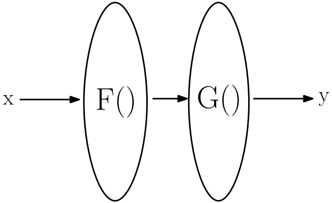
Idea [Poschmann et al., J.Cryptology'11]

Generate S-boxes by combination of others

Decomposition

Idea [Poschmann et al., J.Cryptology'11]

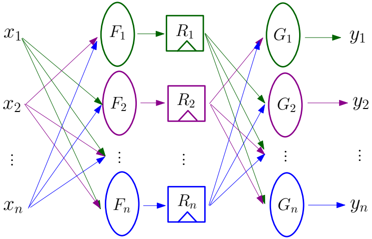
Generate S-boxes by combination of others



Decomposition

Idea [Poschmann et al., J.Cryptology'11]

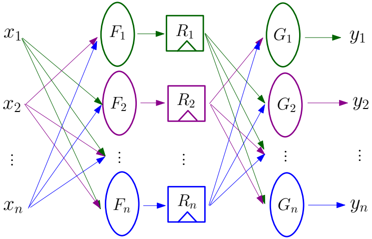
Generate S-boxes by combination of others



Decomposition

Idea [Poschmann et al., J.Cryptology'11]

Generate S-boxes by combination of others



Present S-box (4×4):

Q_{12}	$\times$	Q_{12}
Q_{293}	$\times$	Q_{300}
Q_{294}	$\times$	Q_{299}
Q_{299}	$\times$	Q_{294}
Q_{299}	$\times$	Q_{299}
Q_{300}	$\times$	Q_{293}
Q_{300}	$\times$	Q_{300}

Results

We can share

- All quadratic S-boxes with 3 shares

Results

We can share

- All quadratic S-boxes with 3 shares
- Almost half of the cubic S-boxes with 3 shares with at most 4 decomposition layers

Results

We can share

- All quadratic S-boxes with 3 shares
- Almost half of the cubic S-boxes with 3 shares with at most 4 decomposition layers
- All S-boxes with 4 shares with at most 3 decomposition layers

Results

We can share

- All quadratic S-boxes with 3 shares
- Almost half of the cubic S-boxes with 3 shares with at most 4 decomposition layers
- All S-boxes with 4 shares with at most 3 decomposition layers
- All S-boxes with 5 shares without decomposition

Mathematical Reasoning for Decomposition

Lemma I:

For all $n > 2$, $n \times n$ affine bijections are in A_{2^n}

Lemma II:

All 4×4 quadratic S-boxes are in A_{16}

Mathematical Reasoning for Decomposition

Lemma I:

For all $n > 2$, $n \times n$ affine bijections are in A_{2^n}

Lemma II:

All 4×4 quadratic S-boxes are in A_{16}

Theorem

A 4×4 bijection can be decomposed using quadratic bijections iff it belongs to A_{16}.

$$S_{ixj} = Q_i \circ A \circ Q_j$$

Overview of Classes

Overview of # of classes w.r.t # of shares and layers of decomposition

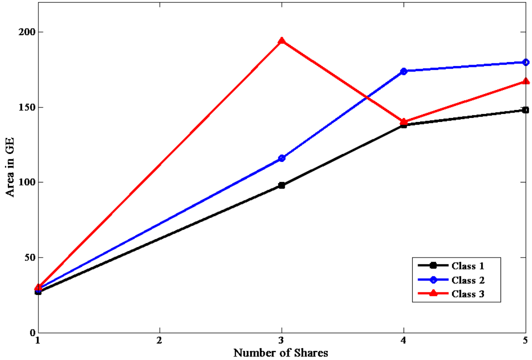
	unshared			3 shares				4 shares			5 shares
# of layers	**1**	**2**	**3**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**1**
quadratic	6			5	1			6			6
cubics in A_{16}		30			28	2			30		30
cubics in A_{16}			114			113	1			114	114
cubics in $S_{16} \setminus A_{16}$		-			-			4	22	125	151

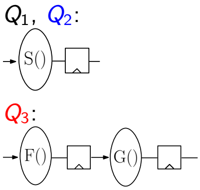
Overview of Classes

Overview of # of classes w.r.t # of shares and layers of decomposition

	unshared			3 shares				4 shares			5 shares
# of layers	**1**	**2**	**3**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**1**
quadratic	6			5	1			6			6
cubics in A_{16}		30			28	2			30		30
cubics in A_{16}			114			113	1			114	114
cubics in $S_{16} \setminus A_{16}$		-				-		4	22	125	151

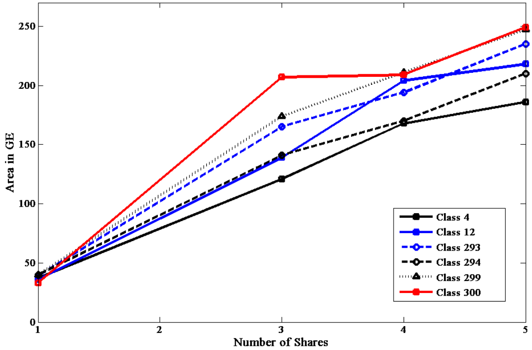
Quadratic 3 × 3 S-boxes





TSMC 0.18μm standard cell library

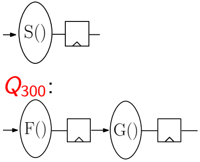
Quadratic 4 × 4 S-boxes



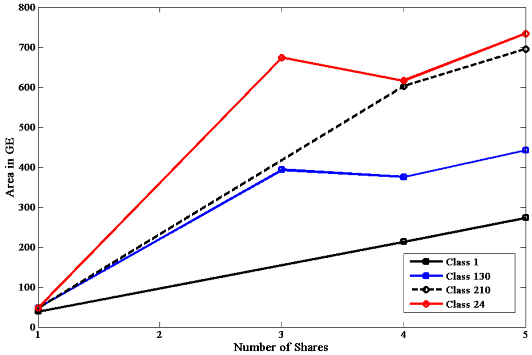
TSMC 0.18μm standard cell library

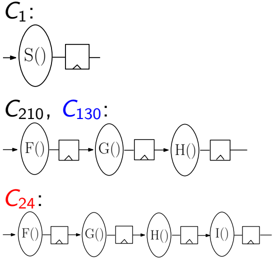
Q_4, Q_{12}, Q_{293}, Q_{294}, Q_{299}:

Q_{300}:



Cubic 4 × 4 S-boxes





TSMC 0.18μm standard cell library

Conclusion

- TI is extended to all 3×3, 4×4 and DES S-boxes

Conclusion

- TI is extended to all 3×3, 4×4 and DES S-boxes
- Number of decomposition layers necessary

Conclusion

- TI is extended to all 3×3, 4×4 and DES S-boxes
- Number of decomposition layers necessary
- Less number of shares does NOT always imply smaller area

Conclusion

- TI is extended to all 3×3, 4×4 and DES S-boxes
- Number of decomposition layers necessary
- Less number of shares does NOT always imply smaller area
- TI can also be efficient

Thank you!