Decomposed S-Boxes and DPA Attacks: A Quantitative Case Study using PRINCE

Ravikumar Selvam, Dillibabu Shanmugam, Suganya Annadurai, Jothi Rangasamy

Society for Electronic Transactions and Security (SETS)

December 17, 2016

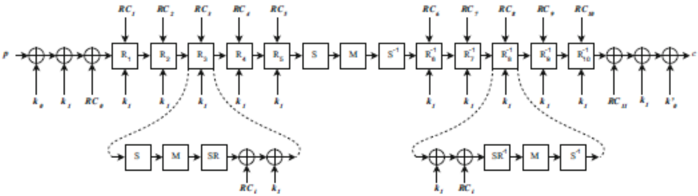
Strategy and Synergy for Security

Outline

- PRINCE and its S-Box decomposition
- Threshold implementation (TI) of decomposed S-Box
- Transparency Order (TO) of decomposed S-box
- Experiment Results (Trade-off Comparison)

PRINCE cipher

PRINCE 64/128: ASIACRYPT2012



Single circuit for both encryption /decryption

Implementation attack on PRINCE

- CPA on round based implementation, CPSS2015
- CPA on unrolled implementation, LightSec2015

Point of attack is S-box

S-Box

- S-Box is a non-linear function
- Provides confusion property
- PRINCE, Golden S-box(G_{13})

Motivation and Contributions

- Adopt existing countermeasure in efficient way
- Identify optimal S-box resistance against DPA from implementation perspective

Countermeasure

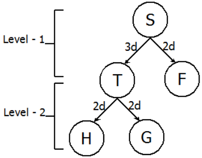
- Threshold implementation (TI) is secure against first order DPA
- Trade-off factors (Area, Latency, Level of Security) need to be considered for resource constrained device.

Threshold Implementation

- TI works on sharing principle, proposed by *Nikova et al*
- No.of shares (S_n) is based on algebraic degree (d) of S-box, that is $S_n \geq$ d + 1 ; $S_n \geq$ 3+1; $S_n \geq$ 4;
- Increases the circuit complexity and its area overhead

Decompose the S-box into smaller functions with lower degree

For PRINCE S-box two level decomposition is possible.



- Functions F,G,H has degree 2, therefore $S_n \geq$ 2+1
- TI requires minimum 3 shares.

Threshold Implementation

Classes(C) and Affines(A) of decomposed S-Box functions

- In first level decomposition, decomposed into one cubic class, one quadratic class and affines, $S = A_3 \circ C_C \circ A_2 \circ C_Q \circ A_1$
- In second level decomposition, cubic class is decomposed into two quadratic classes and affines, $C_C = A_6 \circ C_Q \circ A_5 \circ C_Q \circ A_4$
- $S = A_3 \circ A_6 \circ C_Q \circ A_5 \circ C_Q \circ A_4 \circ A_2 \circ C_Q \circ A_1$

$C_Q = \{4, 12, 293, 294, 299, 300\}$

- Many solutions are possible.
- 644 solutions are taken for analysis

Threshold Implementation

Solutions need to satisfy TI properties for secure shared implementation

- Correctness
- Non-completeness
- Uniformity

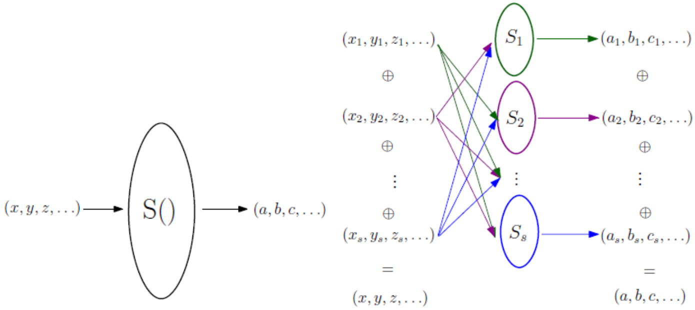


Figure: TI properties

Threshold Implementation

Example: y = f(x) = a AND b

a = (a_1, a_2, a_3); b = (b_1, b_2, b_3);

a = 1; $a_1 = 1, a_2 = 1, a_3 = 1$;

b = 1; $b_1 = 0, b_2 = 1, b_3 = 0$;

y = f(x) = 1.1 = 1;

- Correctness: a = $(a_1 \oplus a_2 \oplus a_3)$; b = $(b_1 \oplus b_2 \oplus b_3)$;
  input side: a = $(1 \oplus 1 \oplus 1) = 1$; b = $(0 \oplus 1 \oplus 0) = 1$;
  output side: $f = f_1 \oplus f_2 \oplus f_3 = 0 \oplus 0 \oplus 1 = 1$
- Non-completeness
  $f_1(a_2, b_2, a_3, b_3) = a_2b_2 \oplus a_2b_3 \oplus a_3b_2 = 1.1 \oplus 1.0 \oplus 1.1 = 0$
  $f_2(a_3, b_3, a_1, b_1) = a_3b_3 \oplus a_3b_1 \oplus a_1b_3 = 1.0 \oplus 1.0 \oplus 1.0 = 0$
  $f_3(a_1, b_1, a_2, b_2) = a_1b_1 \oplus a_1b_2 \oplus a_2b_1 = 1.0 \oplus 1.1 \oplus 1.0 = 1$
- Uniformity
  Input(a,b) = 1.1 the output $f = f_1 \oplus f_2 \oplus f_3 = 1$ and the distribution of its shared output values $(f_1, f_2, f_3) \in \{001, 010, 100, 111\}$ has to be uniform. In other words, each possible shared output has to occur equally likely.

Threshold Implementation

- Need to find an area efficient solution
- *Poschmann et al* proposed a formula to estimate weight sum of shared function.

$$W_{sum} = (2xC) + (6xL) + (27xQ) \quad (1)$$

$$W_{modsum} = 2x((3xC) - 2) + 6x(L + Q - 1) + (21xQ) \quad (2)$$

C = Constant, L = Linear coefficient, Q = quadratic coefficient

Function	Parameters			Weighted Sum		
	C	L	Q	W_{msum}	W_{sum}	W_{modsum}
F=1+x+y+w+xz	1	3	1	41	47	41

$$f_1 = 1 + x_2 + y_2 + w_2 + x_2z_2 + x_2z_3 + x_3z_2$$
$$f_2 = x_3 + y_3 + w_3 + x_3z_3 + x_3z_1 + x_1z_3$$
$$f_3 = x_1 + y_1 + w_1 + x_1z_1 + x_1z_2 + x_2z_1$$

GE for XOR = 2, AND = 1 $\therefore W_{msum} = 16 * (XOR) + 9 * (AND) = 41$

Threshold Implementation

- Area efficient solution has 412 GE.
- Decomposed Sbox Functions F,G,H

Table: S-Box Decomposition

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$F(x)$	0	A	2	8	1	3	B	9	E	5	D	6	F	C	4	7
$G(x)$	E	4	0	A	2	8	C	6	9	7	5	B	D	3	1	F
$H(x)$	3	6	D	8	A	F	4	1	7	2	C	9	0	5	B	E
$S(x) = H(G(F(x)))$	B	F	3	2	A	C	9	1	6	7	8	0	E	5	D	4

- The same procedure is followed to arrive inverse S-box decomposed solution with Functions F^{-1},G^{-1},H^{-1}
- G and G^{-1} functions are same. Therefore, implementation can be optimized further

Functions	F	G	H	Total GE
S-Box	126	123	163	412
Inverse S-Box	97	123	134	354

- Combined & Optimized implementation of S-box and Inv S-box has 643 GE.

Threshold Implementation

ANF form of F(w,x,y,z) [0A2813B9E5D6FC47]
F^1 = x + w*z + w*y
F^2 = z + y + w
F^3 = w
F^4 = z + x*z + x*y + w

ANFs of the PRINCE S-Box decomposition with 3-shares for TI, **F function:**

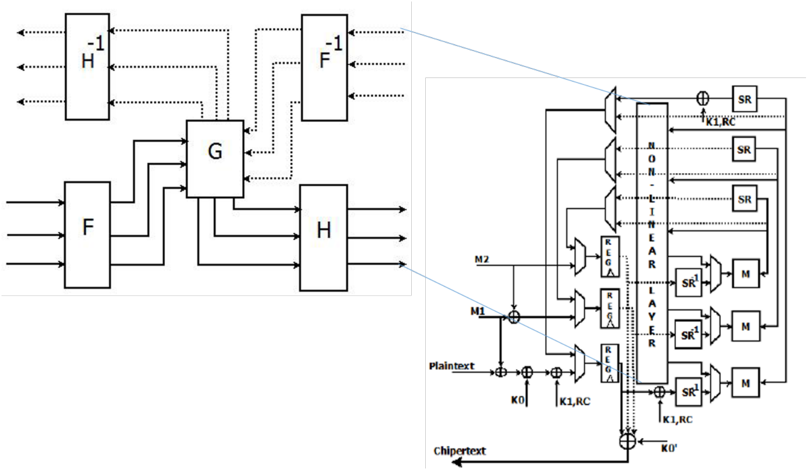
$$F_1(w_2, x_2, y_2, z_2, w_3, x_3, y_3, z_3) = (f_{13}, f_{12}, f_{11}, f_{10})$$
$$f_{10} = x_2 + w_2 y_2 + w_2 y_3 + w_3 y_2 + w_2 z_2 + w_2 z_3 + w_3 z_2$$
$$f_{11} = z_2 + y_2 + w_2$$
$$f_{12} = w_2$$
$$f_{13} = z_2 + w_2 + x_2 z_2 + x_2 z_3 + x_3 z_2 + x_2 y_2 + x_2 y_3 + x_3 y_2$$

$$F_2(w_3, x_3, y_3, z_3, w_1, x_1, y_1, z_1) = (f_{23}, f_{22}, f_{21}, f_{20})$$
$$f_{20} = x_3 + w_3 y_3 + w_3 y_1 + w_1 y_3 + w_3 z_3 + w_3 z_1 + w_1 z_3$$
$$f_{21} = z_3 + y_3 + w_3$$
$$f_{22} = w_3$$
$$f_{23} = z_3 + w_3 + x_3 z_3 + x_3 z_1 + x_1 z_3 + x_3 y_3 + x_3 y_1 + x_1 y_3$$

$$F_3(w_1, x_1, y_1, z_1, w_2, x_2, y_2, z_2) = (f_{33}, f_{32}, f_{31}, f_{30})$$
$$f_{30} = x_1 + w_1 y_1 + w_1 y_2 + w_2 y_1 + w_1 z_1 + w_1 z_2 + w_2 z_1$$
$$f_{31} = z_1 + y_1 + w_1$$
$$f_{32} = w_1$$
$$f_{33} = z_1 + w_1 + x_1 z_1 + x_1 z_2 + x_2 z_1 + x_1 y_1 + x_1 y_2 + x_2 y_1$$

Threshold Implementation

Round based implementation architecture of PRINCE TI.
S-box and Inverse S-box implementation with shared G function.



Threshold Implementation

- To evaluate security of protected implementation. Ported the solution on sasebo G board, target FPGA, Xilinx 2vp7
- Captured 300000 samples power traces for CPA

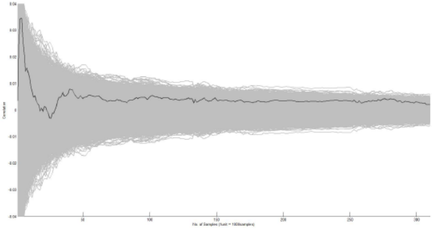


Figure: DPA on decomposed TI

- Figure shows correct key guess is hidden (black waveform) with other key hypothesis.
- TI implementation is resistant against CPA

Transparency Order of decomposed S-box

Optimal S-Box from Implementation perspective

- Identify optimal resistivity of S-Box from implementation perspective
- Transparency order (TO) is a measure to evaluate DPA resistivity of S-Box. TO was proposed by *Prouff et al*
- TO of naive S-Box is not the same as the TO of decomposed S-Box.
- Analyses of TO on decomposed S-Box
  - First level decomposition, no change in TO values.
  - Second level decomposition, has small change in TO values
  - Even small change in TO have significant influence on resistance

Optimal S-Box from Implementation perspective

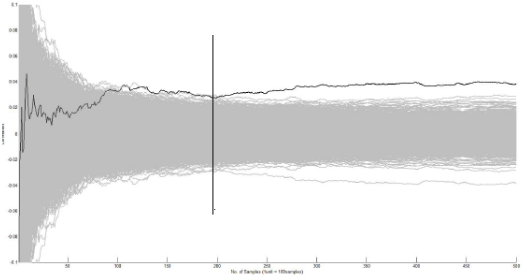
- TO is calculated for 644 solutions
- Sort all solutions based on least TO values
- Estimate GE for sorted solutions.
- Three different cases are taken for analysis
    1. First, Naïve S-box with TO: 3.4
    2. Second, Decomposed quadratic functions F,G,H with different TO values (2.93, 3.2, 3.46)
    3. Third, Decomposed quadratic functions F,G,H with same Least TO value (2.93, 2.93, 2.93).

Experiments

Implement three cases on sasebo G board, target FPGA, Xilinx 2vp7.
Explored Correlation Power Analysis (CPA) on three solutions

Case 1: Naïve S-Box implementation

- TO = 3.4 and GE = 78
- Capture 30,000 power traces for CPA

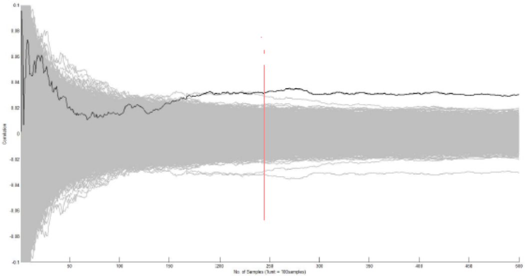


- In plot, correct key(black) guess is above other key hypothesis.
- All bytes of the key are retrieved successfully.

Experiments

Case 2: Decomposed quadratic functions with different TO

- TO F,G,H: (2.93, 3.2, 3.4) and GE = 72
- Captured 30,000 power traces for CPA

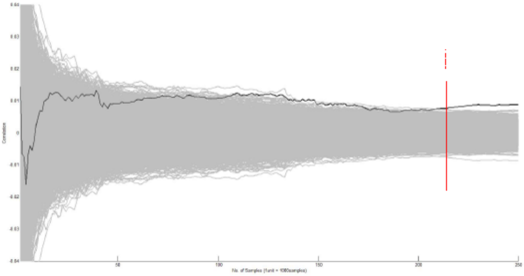


- In plot, correct key(black) guess is above other key hypothesis.
- Retrieved all bytes of the key
- H function TO dominated other functions F,G.

Experiments

Case 3: Decomposed quadratic functions with same TO

- TO F,G,H: (2.93, 2.93, 2.93) and GE = 87
- Captured 2,50,000 power traces for CPA



- In the plot that correct key(black) guess is marginally above other key hypothesis.
- Retrieved 85% of the key
- As TO decreases DPA resistivity of the S-Box increases

Summary

Metrics	Naive	TO	TI
No.of.power-traces for CPA	30,000	2,50,000	$>$ 3,00,000
Area of S-Box in GE	78	87	412

- Level of security : TI $>$ TO $>$ Naïve
- Least TO implementation (with small overhead of GE $=$ 9), achieves 8 times better security compare to Naive.
- **Least TO kind of implementation is recommended for resource constrained device**

Thank You