A Note on 5-bit Quadratic Permutations' Classification

Dušan Božilov Begül Bilgin Hacı Ali Şahin

March 6, 2017

Motivation

- Permutations are main nonlinear part of symmetric primitives
- Quadratic permutations can be used to generate more complex S-boxes
- Affine equivalence preserves several important cryptographic properties
- 5-bit S-boxes: Keccak, Fides, Ascon

Preliminaries

- Algebraic normal form
- Differential distribution table
- Linear approximation table
- Multiplicative complexity
- Uniformity of Threshold Implementations
- Affine equivalence

Algebraic Normal Form

- Given vectorial Boolean function

$$\mathrm{S} = [1\ 0\ 3\ 6\ 5\ 2\ 7\ 4]$$

- Algebraic Normal Form (ANF) of S is given with

$$y_1 = 1 \oplus x_1$$
$$y_2 = x_2 \oplus x_1 x_3$$
$$y_3 = x_1 x_2 \oplus x_3 \oplus x_1 x_3$$

- $\mathrm{S}_{\mathrm{ANF}}$ can be transformed into truth table matrix S_{TT}

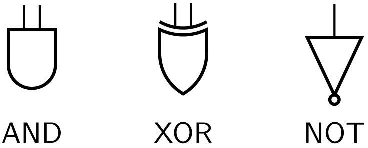
$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

DDT and LAT

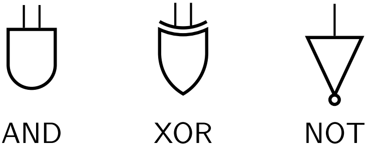
- The difference distribution table (DDT)
  - DDT entries reveal how likely are we to guess output difference for a given input difference
  - The highest value in DDT, δ, is called *differential uniformity*
  - S-boxes that achieve the theoretical minimal δ of 2 are referred to as almost perfect nonlinear (APN) permutations
- The linear approximation table (LAT)
  - LAT entries reveal if linear approximation can be used as a good estimate for given nonlinear S-box
  - The highest value in LAT is denoted by λ
  - If λ achieves theoretical minimum of $2^{(n-1)/2}$, permutation is called an almost bent (AB) permutation

Multiplicative complexity

- Minimal number 2-input AND gates needed for implementation
  - Coarse estimate of the implementation cost



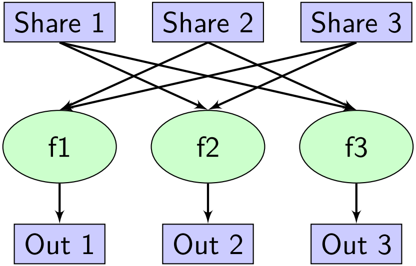
- Minimal number 2-input AND gates needed for implementation
  - Coarse estimate of the implementation cost



- MC is good for estimating cost of applying side-channel protection
  - Larger MC increase the size of protected implementation

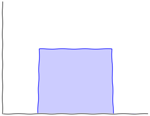
Threshold Implementations

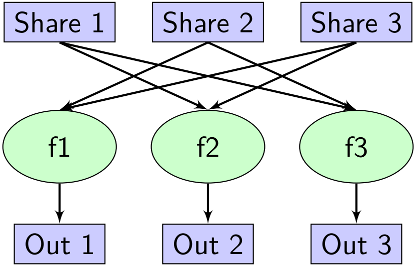
- Boolean masking scheme
  - TI embodies several properties
- Uniformity ensures composability in first order designs



Threshold Implementations

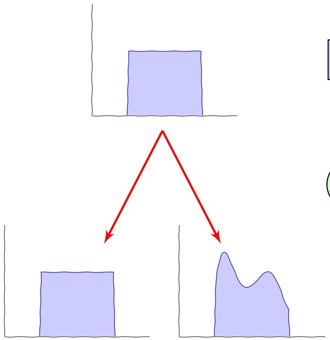
- Boolean masking scheme
  - TI embodies several properties
- Uniformity ensures composability in first order designs

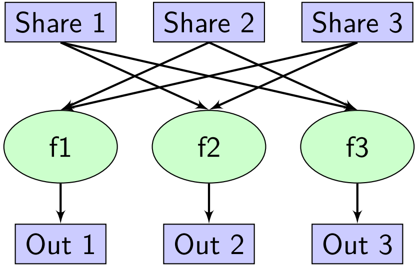




Threshold Implementations

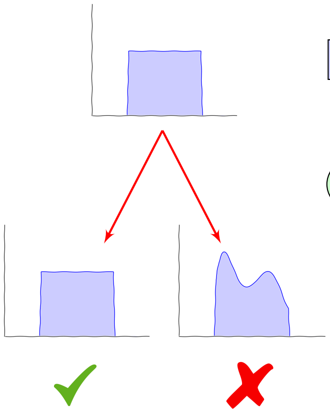
- Boolean masking scheme
  - TI embodies several properties
- Uniformity ensures composability in first order designs

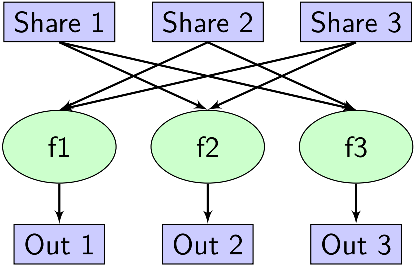




Threshold Implementations

- Boolean masking scheme
  - TI embodies several properties
- Uniformity ensures composability in first order designs





Affine equivalence

- $S' = A \circ S \circ B$
- Permutations that are affine equivalent form an equivalence class
- Affine equivalence preserves linear and differential properties
- There is an average $O(2^{3n})$ complexity algorithm to find affine representative of a class discovered by De Cannière
- For every $n-$bit permutation S there is a permutation S' where $S'(x) = x, x \in \{0, 1, 2, 4, \dots, 2^{n-1}\}$ such that S and S' are affine equivalent
- Affine equivalence classification is exponential problem
    - Boolean functions of up to 6 bits are classified
    - 3-bit and 4-bit permutations classified

Search strategy for 5-bit quadratic permutations

- We focus only on coefficients that are linear or quadratic
- Using previous results from Leander and Poschmann we can fix several columns in S_{ANF}
- For one bit Boolean function all affine equivalence classes are of the form

$$y = x_i \oplus a x_j x_k \oplus b x_m x_n$$

  - We limit number of quadratics in the first row using this constraint
- Balancedness enforced for each row, and any combination of rows

Search strategy for 5-bit quadratic permutations

$$\begin{pmatrix}
c_{1,1} & c_{1,2} & c_{1,3} & c_{1,4} & c_{1,5} & c_{1,6} & c_{1,7} & c_{1,8} & c_{1,9} & c_{1,10} & c_{1,11} & c_{1,12} & c_{1,13} & c_{1,14} & c_{1,15} \\
c_{2,1} & c_{2,2} & c_{2,3} & c_{2,4} & c_{2,5} & c_{2,6} & c_{2,7} & c_{2,8} & c_{2,9} & c_{2,10} & c_{2,11} & c_{2,12} & c_{2,13} & c_{2,14} & c_{2,15} \\
c_{3,1} & c_{3,2} & c_{3,3} & c_{3,4} & c_{3,5} & c_{3,6} & c_{3,7} & c_{3,8} & c_{3,9} & c_{3,10} & c_{3,11} & c_{3,12} & c_{3,13} & c_{3,14} & c_{3,15} \\
c_{4,1} & c_{4,2} & c_{4,3} & c_{4,4} & c_{4,5} & c_{4,6} & c_{4,7} & c_{4,8} & c_{4,9} & c_{4,10} & c_{4,11} & c_{4,12} & c_{4,13} & c_{4,14} & c_{4,15} \\
c_{5,1} & c_{5,2} & c_{5,3} & c_{5,4} & c_{5,5} & c_{5,6} & c_{5,7} & c_{5,8} & c_{5,9} & c_{5,10} & c_{5,11} & c_{5,12} & c_{5,13} & c_{5,14} & c_{5,15}
\end{pmatrix}$$

Search strategy for 5-bit quadratic permutations

$$\begin{pmatrix} 1 & 0 & c_{1,3} & 0 & c_{1,5} & c_{1,6} & 0 & c_{1,8} & c_{1,9} & c_{1,10} & 0 & c_{1,12} & c_{1,13} & c_{1,14} & c_{1,15} \\ 0 & 1 & c_{2,3} & 0 & c_{2,5} & c_{2,6} & 0 & c_{2,8} & c_{2,9} & c_{2,10} & 0 & c_{2,12} & c_{2,13} & c_{2,14} & c_{2,15} \\ 0 & 0 & c_{3,3} & 1 & c_{3,5} & c_{3,6} & 0 & c_{3,8} & c_{3,9} & c_{3,10} & 0 & c_{3,12} & c_{3,13} & c_{3,14} & c_{3,15} \\ 0 & 0 & c_{4,3} & 0 & c_{4,5} & c_{4,6} & 1 & c_{4,8} & c_{4,9} & c_{4,10} & 0 & c_{4,12} & c_{4,13} & c_{4,14} & c_{4,15} \\ 0 & 0 & c_{5,3} & 0 & c_{5,5} & c_{5,6} & 0 & c_{5,8} & c_{5,9} & c_{5,10} & 1 & c_{5,12} & c_{5,13} & c_{5,14} & c_{5,15} \end{pmatrix}$$

Up to two nonzero quadratic terms

$$\begin{pmatrix} 1 & 0 & c_{1,3} & 0 & c_{1,5} & c_{1,6} & 0 & c_{1,8} & c_{1,9} & c_{1,10} & 0 & c_{1,12} & c_{1,13} & c_{1,14} & c_{1,15} \\ 0 & 1 & c_{2,3} & 0 & c_{2,5} & c_{2,6} & 0 & c_{2,8} & c_{2,9} & c_{2,10} & 0 & c_{2,12} & c_{2,13} & c_{2,14} & c_{2,15} \\ 0 & 0 & c_{3,3} & 1 & c_{3,5} & c_{3,6} & 0 & c_{3,8} & c_{3,9} & c_{3,10} & 0 & c_{3,12} & c_{3,13} & c_{3,14} & c_{3,15} \\ 0 & 0 & c_{4,3} & 0 & c_{4,5} & c_{4,6} & 1 & c_{4,8} & c_{4,9} & c_{4,10} & 0 & c_{4,12} & c_{4,13} & c_{4,14} & c_{4,15} \\ 0 & 0 & c_{5,3} & 0 & c_{5,5} & c_{5,6} & 0 & c_{5,8} & c_{5,9} & c_{5,10} & 1 & c_{5,12} & c_{5,13} & c_{5,14} & c_{5,15} \end{pmatrix}$$

Search strategy for 5-bit quadratic permutations

Up to two nonzero quadratic terms

$$\begin{pmatrix}
1 & 0 & c_{1,3} & 0 & c_{1,5} & c_{1,6} & 0 & c_{1,8} & c_{1,9} & c_{1,10} & 0 & c_{1,12} & c_{1,13} & c_{1,14} & c_{1,15} \\
0 & 1 & c_{2,3} & 0 & c_{2,5} & c_{2,6} & 0 & c_{2,8} & c_{2,9} & c_{2,10} & 0 & c_{2,12} & c_{2,13} & c_{2,14} & c_{2,15} \\
0 & 0 & c_{3,3} & 1 & c_{3,5} & c_{3,6} & 0 & c_{3,8} & c_{3,9} & c_{3,10} & 0 & c_{3,12} & c_{3,13} & c_{3,14} & c_{3,15} \\
0 & 0 & c_{4,3} & 0 & c_{4,5} & c_{4,6} & 1 & c_{4,8} & c_{4,9} & c_{4,10} & 0 & c_{4,12} & c_{4,13} & c_{4,14} & c_{4,15} \\
0 & 0 & c_{5,3} & 0 & c_{5,5} & c_{5,6} & 0 & c_{5,8} & c_{5,9} & c_{5,10} & 1 & c_{5,12} & c_{5,13} & c_{5,14} & c_{5,15}
\end{pmatrix}$$

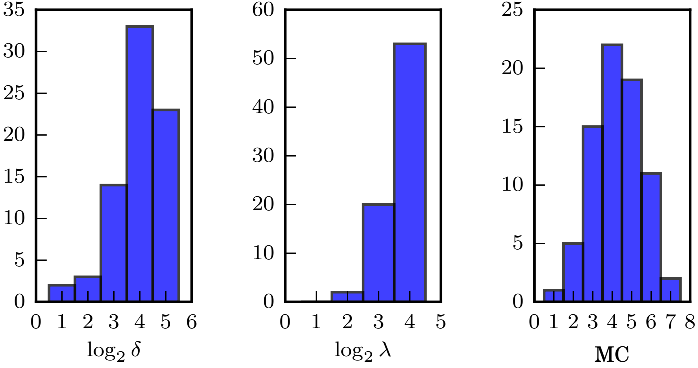
- 10 balanced functions for the first row, 472 for each of the other rows
- Checking balancedness for combinations of all rows, we construct a bit over than 10 million $\sim \mathrm{O}(2^{24})$ candidates
- We find representatives of all candidates and remove duplicates

Results

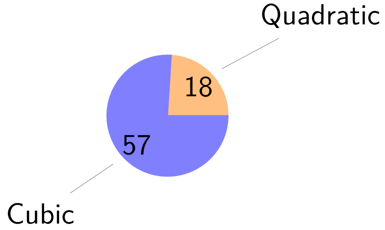
- 75 classes
- Two almost bent classes (δ: 2, λ: 4)
- 12 classes as good as Keccak S-box(δ: 8, λ: 8)
- Three non-AB classes with smaller differential uniformity than Keccak S-box (δ: 4, λ: 8)

Results

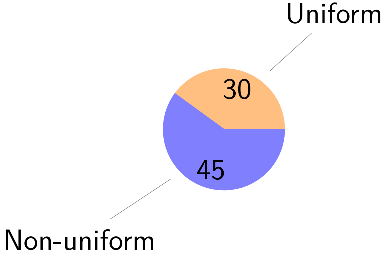
- 75 classes
- Two almost bent classes (δ: 2, λ: 4)
- 12 classes as good as Keccak S-box(δ: 8, λ: 8)
- Three non-AB classes with smaller differential uniformity than Keccak S-box (δ: 4, λ: 8)



- Algebraic degree of the inverse permutation



- Uniform Threshold Implementations with three shares



Future work

- Improvements for 6-bit quadratic permutations
  - Current algorithm estimated at $\approx \mathrm{O}(2^{70})$ permutations to investigate
- Adapting for non-quadratic classes
- Exploring possible compositions that can be obtained from the 75 quadratic classes

Thank you! Questions?