Radboud University

Thinking Outside the Superbox

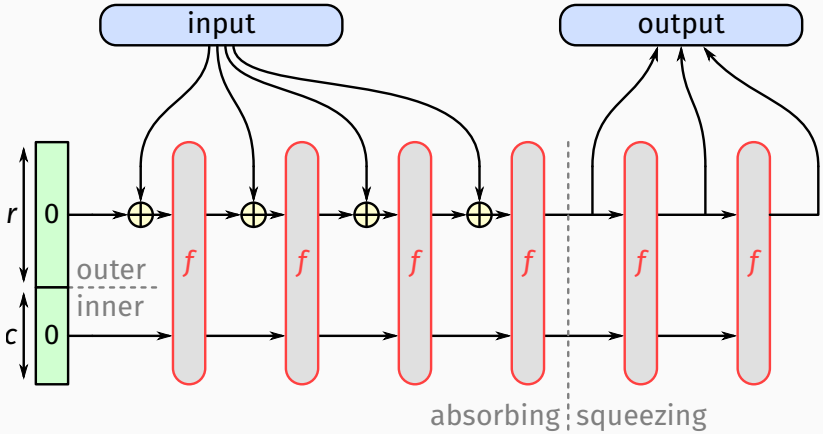
Nicolas Bordes[1], Joan Daemen[2], Daniël Kuijsters[2], Gilles Van Assche[3]

Crypto 2021

[1]Université Grenoble Alpes (France)
[2]Radboud University (The Netherlands)
[3]STMicroelectronics (Belgium)

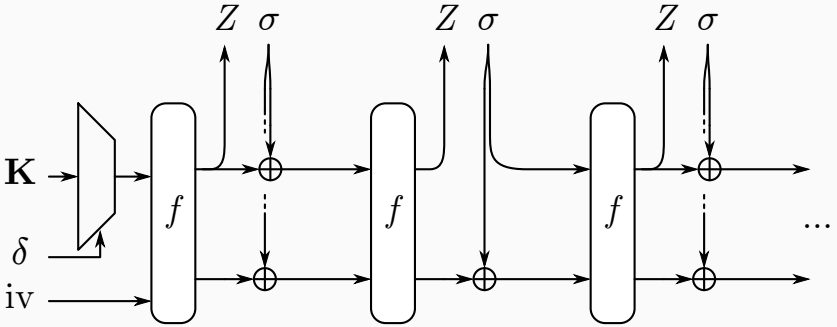
ESCADA

The Sponge Construction [Bertoni et al., Eurocrypt 2008]

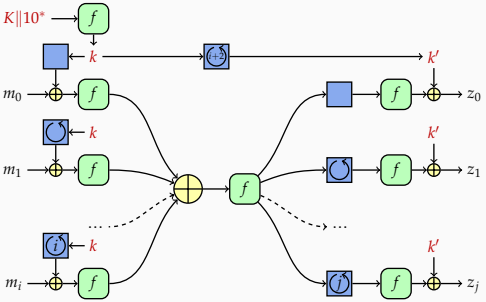


Proven secure if f is a randomly and uniformly chosen permutation

Keyed Duplex [Bertoni et al., SAC 2011]



Proven secure if f is a randomly and uniformly chosen permutation



- In practice we build permutations that (try to) withstand cryptanalysis of the scheme
- Study round-reduced versions using knowledge of inner structure

Research Question

Research question: How do different designs of cryptographic permutations affect (differential) cryptanalysis?

Given a permutation f:

- An input difference a through f giving an output difference b
  $\rightsquigarrow (a, b)$ called a differential
- Divide $\#\{x \mid f(x) + f(x + a) = b\}$ by the total number of different x
  $\rightsquigarrow$ Differential Probability (DP) of (a, b)
- Often $-\log_2(\mathrm{DP}(a, b))$ is more convenient to work with
  $\rightsquigarrow$ weight of (a, b)

The Structure We Have Considered

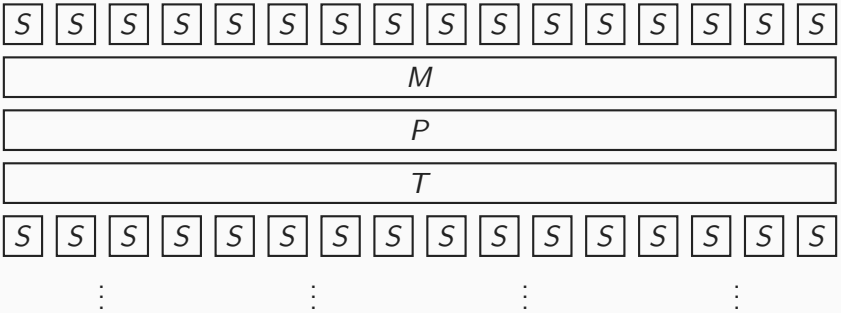
Permutations built as the composition of r round functions of the form $T \circ L \circ N$ where:

- N is an S-box layer, i.e., it can be written as $N = S \times \cdots \times S$
- L is a linear layer that is the composition of a mixing layer M (possibly the identity) and a shuffle layer P (a bit permutation)
- T is an addition of a constant, i.e., a translation

Typically, L and N are the same for each round

We do not consider Feistel structures or ARX-based round functions

The Structure We Have Considered (2)



Differential Trails

A more precise description of how differences propagate through a permutation:

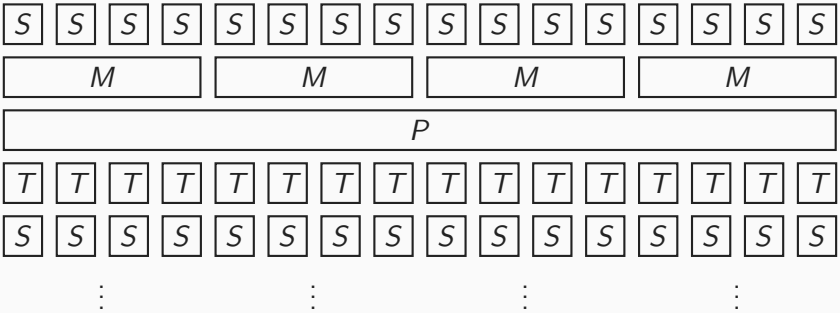
- $(r+1)$-tuple $(q_0, \ldots, q_r)$ of intermediate differences in f
  $\rightsquigarrow$ called a differential trail (AKA characteristic)
- Number of input pairs that follow each difference of the trail divided by the total number of different pairs $\rightsquigarrow$ DP of the differential trail
- Sum of the weights of the differentials over active S-Boxes $\rightsquigarrow$ weight of the differential trail
- Differentials trails with DP > 0 that share q_0 and q_r $\rightsquigarrow$ clustering of trails

An Aligned Approach

The central notion in the paper, alignment:

- Coined in [Bertoni et al., Ecrypt II Hash 2011] (But different from our definition)
- Bits grouped along S-box boundaries, e.g., in nibbles or bytes
- When consistently processed in these groups $\rightsquigarrow$ we call round function aligned
- Naturally leads to the concept of a superbox substructure
- This, combined with an MDS matrix, allows for reasoning about differential properties using combinatorial arguments

An Aligned Approach (2)



An Unaligned Approach

- An unaligned approach avoids such grouping in the design of round functions
- Needs computer programs to investigate trail bounds
- Superficially, one might wonder why not every cipher is designed with an aligned approach
- . . . but an aligned approach may have (potentially unwanted?) side-effects

Our contribution $\rightsquigarrow$ trying to quantify these side-effects

Ciphers Considered

	Aligned	Mixing	S-box size	# S-boxes	Width
Rijndael	yes	strong	8	32	256
Saturnin	yes	strong	4	64	256
Spongent	yes	weak	4	96	384
Xoodoo	no	strong	3	128	384

We want *you* to increase the sample size!

Software available at: `https://github.com/ongetekend/ThinkingOutsideTheSuperbox`

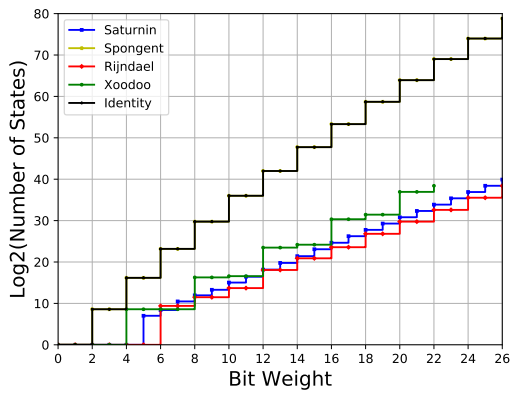
Branch Number

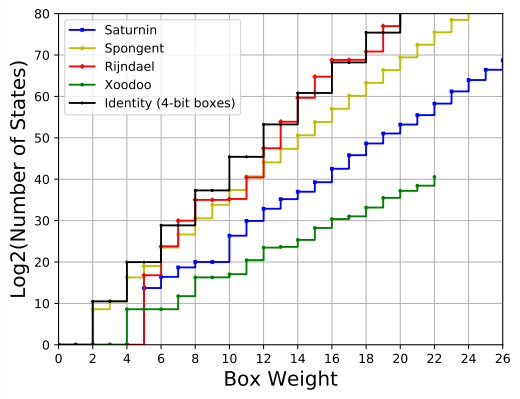
- The DP of a trail can be approximated by the product of DPs of *active* S-boxes
- A trail has a low DP if few S-boxes are active or the S-boxes have a high DP
- Wide trail strategy [Daemen, PhD thesis 1995]: ensure that all trails have many active S-boxes
- Accomplish this by choosing the mixing layer M such that:
  - Few active S-boxes in a give many active S-boxes in $M(a)$
  - Few active S-boxes in b give many active S-boxes in $M^{-1}(b)$
- The branch number [Daemen, PhD thesis 1995] of M is defined as

$$\min_{a \neq 0} \{ w_\Pi(a) + w_\Pi(M(a)) \},$$

where $w_\Pi(\cdot)$ is the *box* weight, i.e., it counts the number of active S-boxes

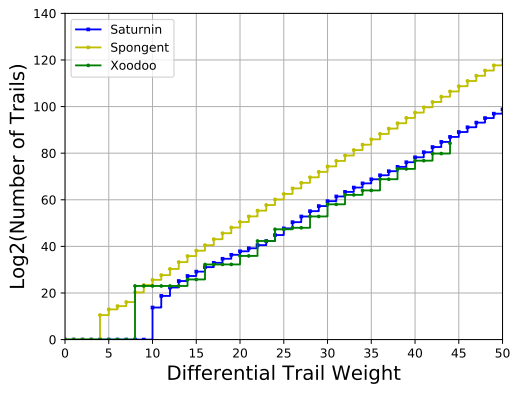
Huddling – Two-round Bit and Box Weight Histograms

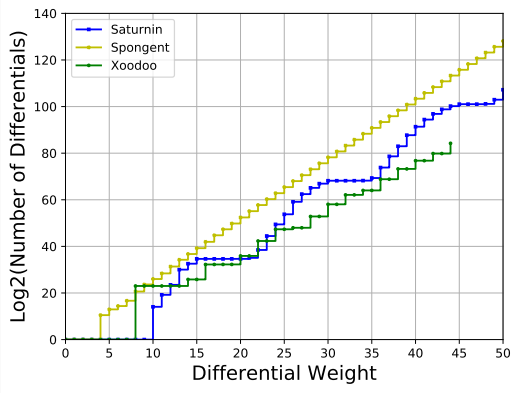




- We see a loss of diffusion in going from bit to box weight $\rightsquigarrow$ huddling
- Huddling increases with S-box size $\rightsquigarrow$ more pronounced in aligned ciphers

Clustering – Two-round Differential and Trail Weight Histograms





We see that trails cluster together in differentials

Further Contributions

- Two-round histograms of the linear propagation properties
- Three-round trail histograms of SATURNIN and XOODOO
- We have studied the independence of round differentials for three rounds of XOODOO
- Based on available information, we sketched what happens when considering weight histograms of four rounds and beyond

Conclusion

Given the same resources $\rightsquigarrow$ XOODOO performs best w.r.t. differential and linear propagation properties

Thank you for your attention!

Part of this work was sponsored by ERC grant ESCADA