Skipjack's F-Table and S-Box Fun

Alex Biryukov, Léo Perrin

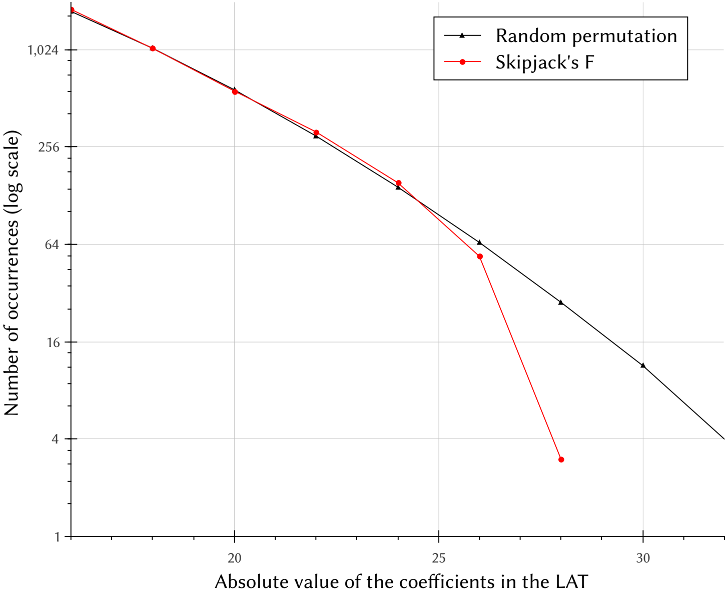
SnT, University of Luxembourg

FSE 2015 Rump Session

Skipjack's F Is Not Good...

		Skipjack	Random	AES
Diff. Spec.	0	38849	39252	32640
	2	20559	19962	32130
	4	4855	4875	255
	6	686	827	0
	8	69	99	0
	10	5	9	0
	12	2	1	0
$\max_{a,b\geq 1}\{\ell_{a,b}\}$		28	32	16

But Skipjack's F Doesn't Look Random Either!



Actually, Skipjack's F Certainly Isn't Random

- Low highest $\ell_{a,b}$:

$$P[\ell_{a,b} \leq 28 \text{ (always)}] \approx 2^{-25.6}$$

Actually, Skipjack's F Certainly Isn't Random

- Low highest $\ell_{a,b}$:

$$P[\ell_{a,b} \leq 28 \text{ (always)}] \approx 2^{-25.6}$$

- Low number of occurrences of highest $\ell_{a,b}$

$$P[\ell_{a,b} = 28 \text{ at most 3 times}] \approx 2^{-54.4}$$

Actually, Skipjack's F Certainly Isn't Random

- Low highest $\ell_{a,b}$:

$$P[\ell_{a,b} \leq 28 \text{ (always)}] \approx 2^{-25.6}$$

- Low number of occurrences of highest $\ell_{a,b}$

$$P[\ell_{a,b} = 28 \text{ at most 3 times}] \approx 2^{-54.4}$$

1. F not picked uniformly at random.

Actually, Skipjack's F Certainly Isn't Random

- Low highest $\ell_{a,b}$:

$$P[\ell_{a,b} \leq 28 \text{ (always)}] \approx 2^{-25.6}$$

- Low number of occurrences of highest $\ell_{a,b}$

$$P[\ell_{a,b} = 28 \text{ at most 3 times}] \approx 2^{-54.4}$$

1. F not picked uniformly at random.
2. F not picked (using some criteria) within a set of random S-Boxes.

Actually, Skipjack's F Certainly Isn't Random

- Low highest $\ell_{a,b}$:

$$P[\ell_{a,b} \leq 28 \text{ (always)}] \approx 2^{-25.6}$$

- Low number of occurrences of highest $\ell_{a,b}$

$$P[\ell_{a,b} = 28 \text{ at most 3 times}] \approx 2^{-54.4}$$

1. F not picked uniformly at random.
2. F not picked (using some criteria) within a set of random S-Boxes.
3. Whatever was done improved the linear properties.

Actually, Skipjack's F Certainly Isn't Random

- Low highest $\ell_{a,b}$:

$$P[\ell_{a,b} \leq 28 \text{ (always)}] \approx 2^{-25.6}$$

- Low number of occurrences of highest $\ell_{a,b}$

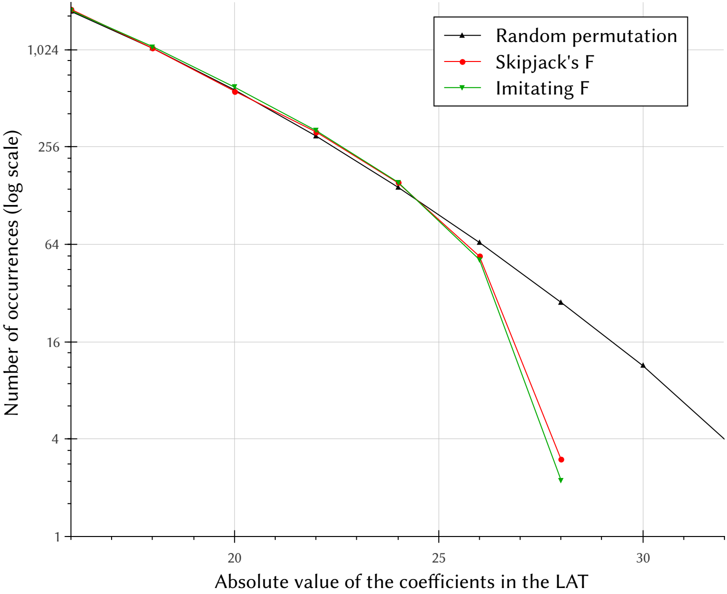
$$P[\ell_{a,b} = 28 \text{ at most 3 times}] \approx 2^{-54.4}$$

1. F not picked uniformly at random.
2. F not picked (using some criteria) within a set of random S-Boxes.
3. Whatever was done improved the linear properties.

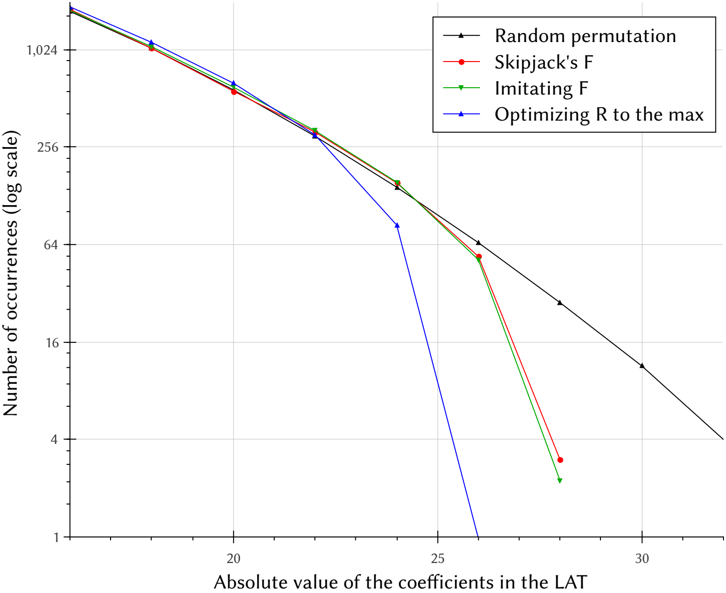
- Let us optimize for this quantity:

$$R = \sum_{(a,b) \in [1,255]^2} 2^{|\ell_{a,b}|}$$

The Imitation Game



The Optimization Game



Pictures for S-Box Analysis

And now for something...

Pictures for S-Box Analysis

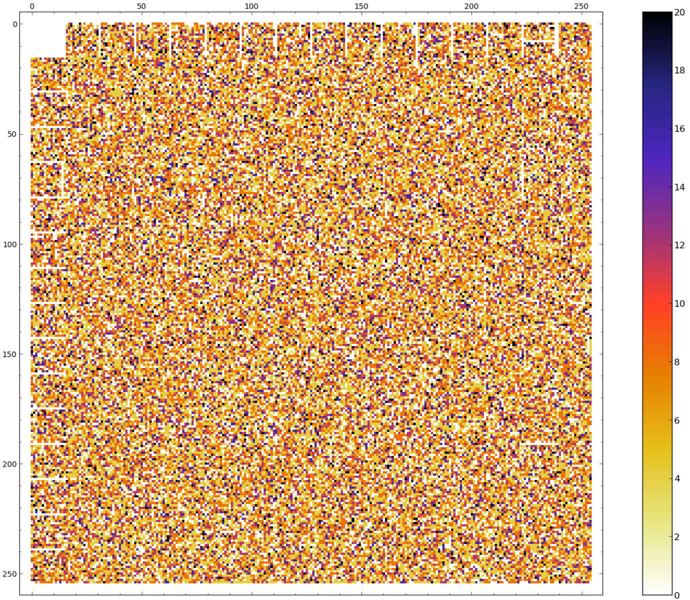
And now for something...
... somewhat related.

Pictures for S-Box Analysis

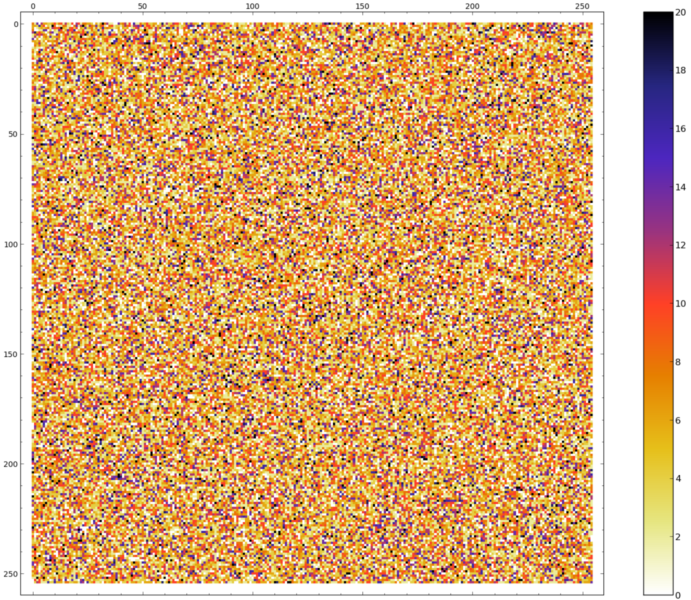
And now for something...
... somewhat related.

Modern Art to the cryptographer's rescue!

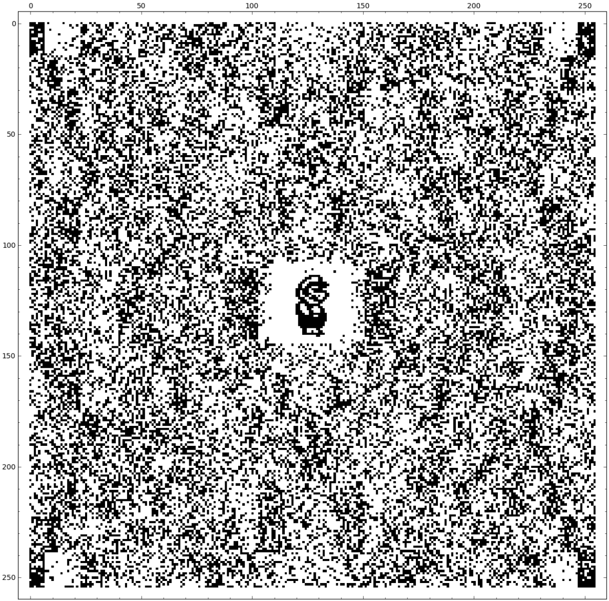
CLEFIA's S_0's LAT, JP style



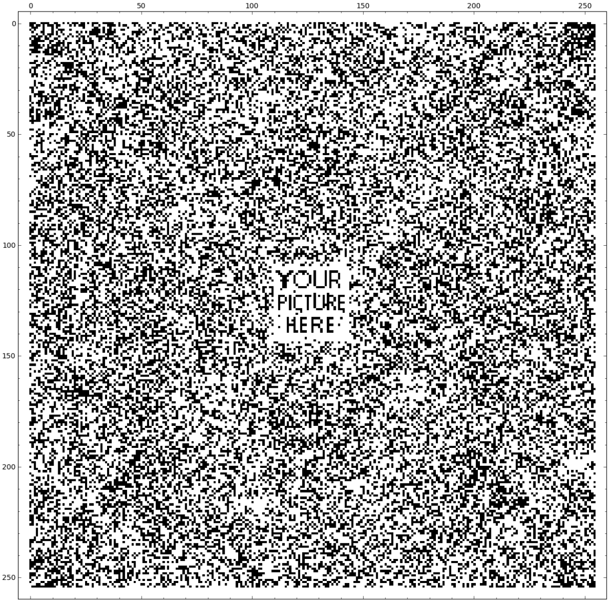
Skipjack's S-Box's LAT, JP style



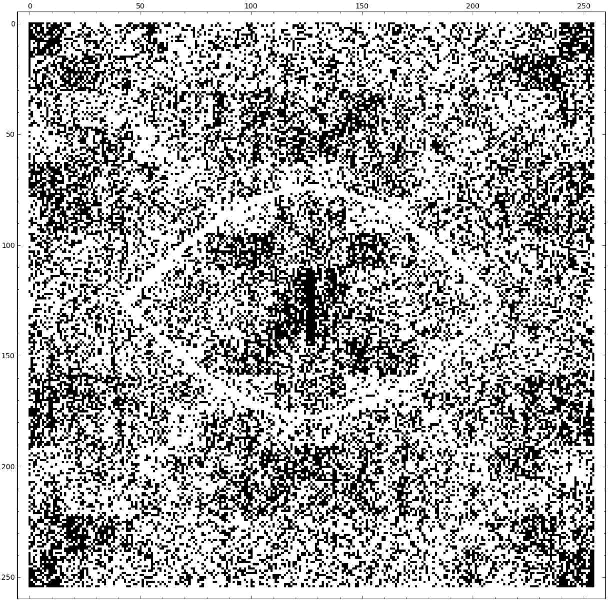
From a Picture to a S-Box



Embedding Your Own Picture in a DDT



A Possible Replacement for Skipjack's F-Table



Conclusion