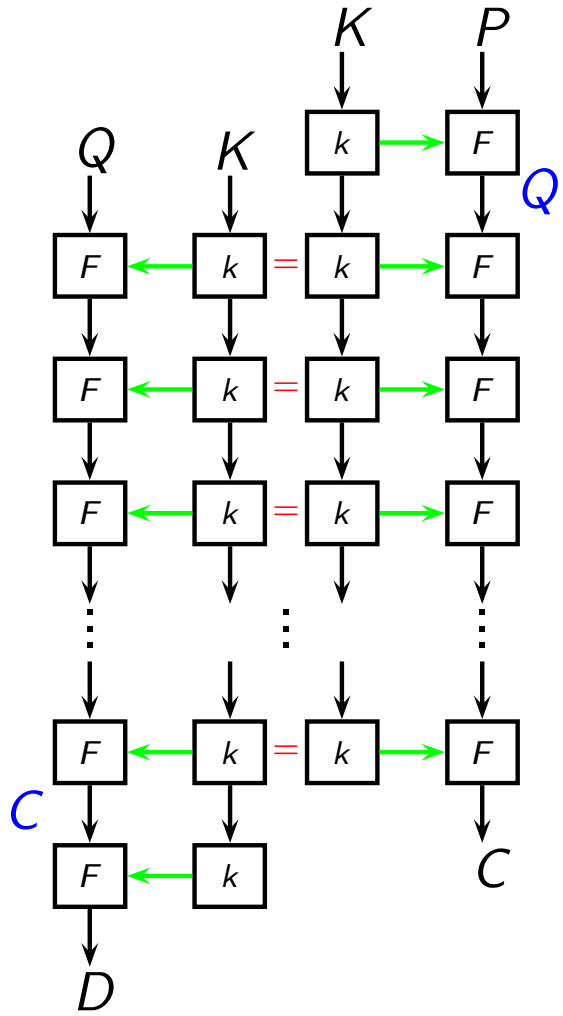
New Slide Attacks on Almost Self-Similar Ciphers

Orr Dunkelman, Nathan Keller,
Noam Lasry, Adi Shamir

May 21th, 2019

Slide Attacks [BW99]

- Presented by Biryukov and Wagner in 1999
- Can be applied to ciphers with the same keyed permutation
- Independent of the number of rounds of the cipher



Slide Attacks [BW99] (cont.)

- Slid pair satisfies

$$\begin{cases} Q = f_k(P), \\ D = f_k(C), \end{cases} \tag{1}$$

- Slide attacks:
  - Find such a slid pair,
  - Use slid pair to extract key.

Extensions and Generalizations

- Slide with twist [BW00]
- Advanced slide [BW00]
- Chains [F01]
- Slidex [DKS12]
- Reflection [K08]
- Quantum [B+18]

Applications

- 1K-DES, 2K-DES, 4K-DES ([BW99,BW00])
- 3K-DES ([B+17])
- 1K-AES ([B+17])
- KeeLoq ([I+08,C+08])
- FF3 ([DV17,HMT19])
- ...

Basic Assumptions

1. All round functions are the same

Basic Assumptions

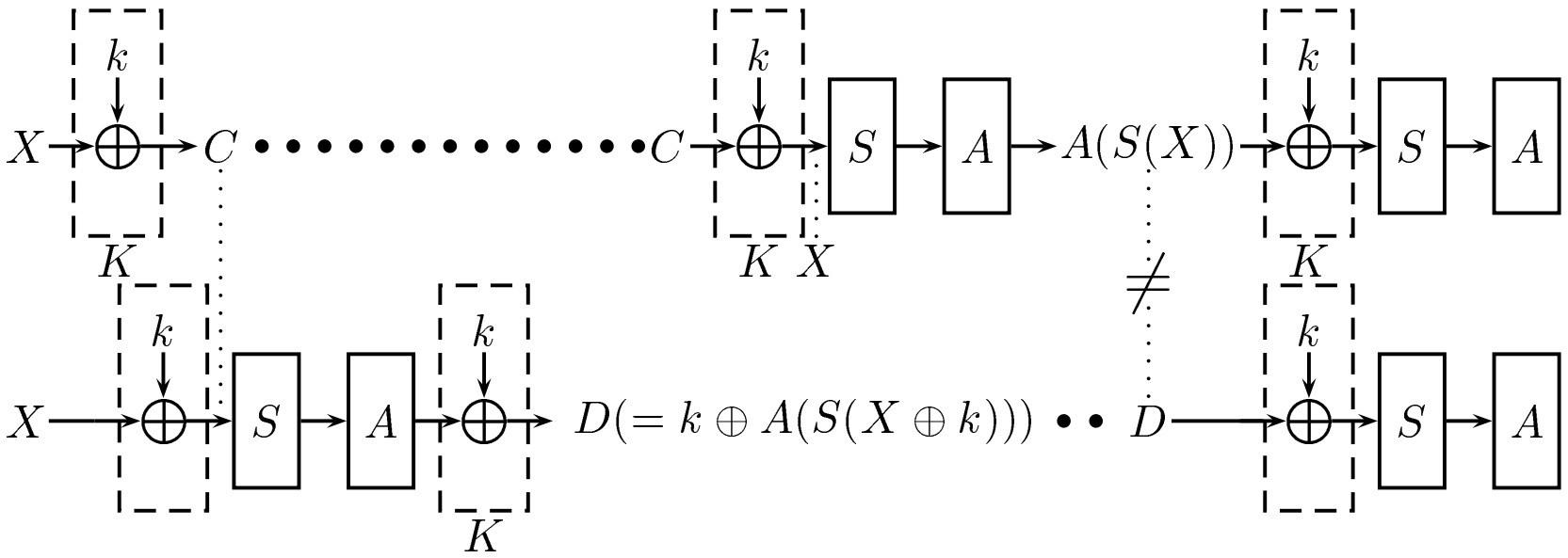
1. All round functions are the same
2. Because of 1, it is possible to iterate and generate more slid pairs

Basic Assumptions

1. All round functions are the same
2. Because of 1, it is possible to iterate and generate more slid pairs

Problem: in AES the last round is different!

Last Round Function ⇒ No Slid Chains



Overcoming the Last Round

Overcoming the Last Round

Introducing **4** new slide techniques:

Overcoming the Last Round

Introducing **4** new slide techniques:

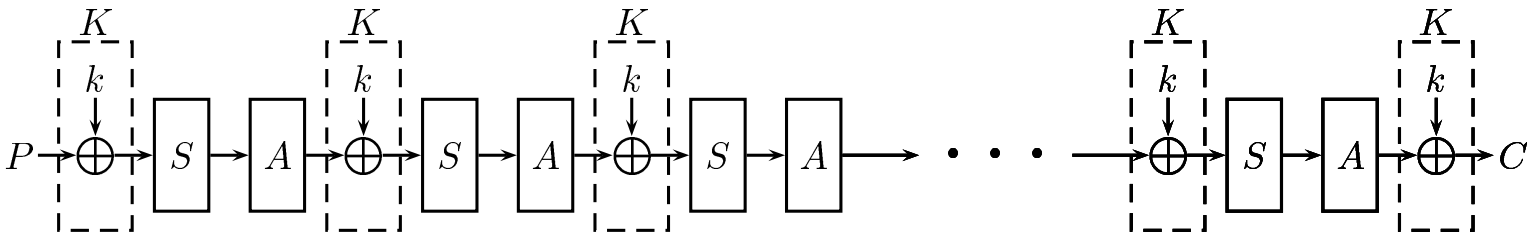
- Slid Sets
- Hypercube of slid pairs
- Suggestive plaintext structures
- Substitution slide

Slid Sets

- Two sets of λ-structures $\{\mathcal{P}\}$ and $\{\mathcal{Q}\}$ such that

$$f_k(\{\mathcal{P}\}) = \{\mathcal{Q}\}$$

- Cool detection techniques!
- Can be used to attack 2K-AES with complexity 2^{68}
- General 2-KSA — $2^{(n+s)/2}$
- Can be used to attack 1K-AES with secret S-boxes with complexity $2^{70.3}$



Results

Cipher	Technique	Complexity (general)		AES-like	
		Data/Memory	Time	Data/Memory	Time
Known S-Boxes					
1-KSAf	Slide [B+17]	$2^{n/2}$ (KP)	$2^{n/2}$	2^{64} (KP)	2^{64}
1-KSAt	Suggestive str.	$3 \cdot 2^{n/2}$ (CP)	$4 \cdot 2^{n/2}$	$2^{65.6}$ (CP)	2^{66}
1-KSAt	Sub. slide	$2^{n/2}$ (KP)	$2^{3n/4}$	2^{64} (KP)	2^{96}
2-KSAf	Slid sets	$2^{(n+s)/2+1}$ (CP)	$2^{(n+s)/2+1}$	2^{69} (CP)	2^{69}
2-KSAf	Slide + Key Guessing	$(n/s)2^{n/2}$ (CP)	$2^{n/2+s}$	2^{68} (CP)	2^{72}
2-KSAtpi †	Slid sets	$2^{(n+m)/2+1}$ (CP)	$\max\{2^{(n+m)/2+1}, 2^{2m}\}$	2^{78} (CP)	2^{78}
3-KSAfi †	Slid sets	$2^{(n+m)/2+1}$ (CP)	$\max\{2^{(n+m)/2+1}, 2^{2m}\}$	2^{81} (CP)	2^{81}
Secret S-Boxes					
1-KSAf	Slid sets	$1.17\sqrt{s}2^{(n+s)/2}$ (CP)	$1.17\sqrt{s}2^{(n+s)/2}$	$2^{70.3}$ (CP)	$2^{70.3}$
1-KSAf	Hypercube	$\sqrt{s}2^{n/2+s(s+3)/4+1}$ (CP)	$\sqrt{s}2^{n/2+s(s+3)/4+1}$	2^{88} (CP)	2^{88}

KP – Known Plaintext; CP – Chosen Plaintext; For AES-like $n = 128, s = 8$

† – this version has incomplete diffusion layer, m denotes the "word" size of the linear operation.

‡ – the memory complexity of this attack is 2^{47}.

Thank you for your Attention!

https://eprint.iacr.org/2019/059

A Formal Complaint: Wrongful Rejection from Rump Session

Orr Dunkelman

May 21th, 2019

Facts

- Eran Lambooij and me wanted to give another rump session presentation

Facts

- Eran Lambooij and me wanted to give another rump session presentation
- As you can see, it is not in the schedule

Facts

- Eran Lambooij and me wanted to give another rump session presentation
- As you can see, it is not in the schedule
- The fact that **we missed** the deadline by **13 hours and 27 minutes** seems to be of little relevance!

(Rump) Session Hijacking Attack

- New attack against timing constraints!

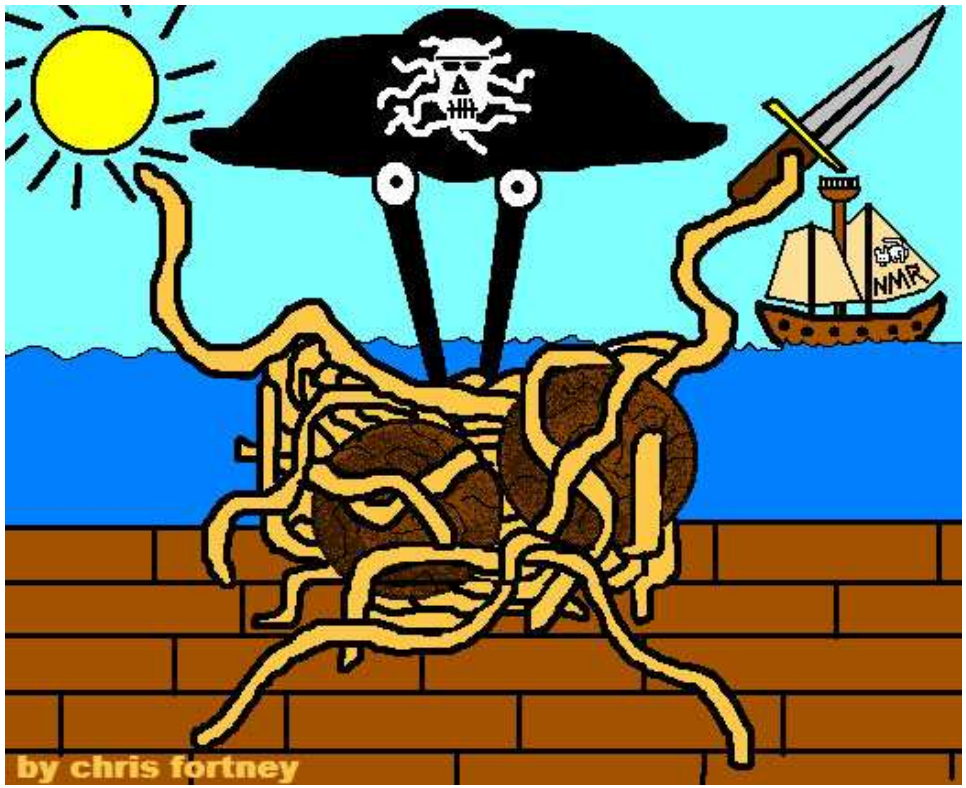
(Rump) Session Hijacking Attack

- New attack against timing constraints!
- CaML + (rump session talk) MR + Time-Travel attack

(Rump) Session Hijacking Attack

- New attack against timing constraints!
- CaML + (rump session talk) MR + Time-Travel attack
- Also works in the "wrong time zone" model

Thank you for your Support!



A Practical Cryptanalysis Competition

A Cycling Approach

Orr Dunkelman and Eran Lambooij

Eurocrypt, Rumpsession, 2019

What do Cryptographers like the Most?

What do Cryptographers like the Most?

Blockchain

What do Cryptographers like the Most?

~~BlockKette~~

Free Drinks

What do Cryptographers like the Most?

~~BlockKette~~

Competitions!

~~Freie Getränke~~

The practical LWC competition

Yellow

Most broken ciphers.

Green

Most points.

Polka dot

Highest broken rounds.

What can **you** do?

- Go to the competition website:
  `https://cryptanex.hideinplainsight.io/lwc/`
- Compute key
- Celebrate
- Submitters - you can help us (contact Eran)