Cryptanalysis of AES-PRF and Its Dual

Patrick Derbez[1] Tetsu Iwata[2] Ling Sun[3,4] Siwei Sun[5]
Yosuke Todo[6] Haoyang Wang[4] Meiqin Wang[3]

1. Univ Rennes, CNRS, IRISA, France
2. Nagoya University, Japan
3. Shandong University, China
4. Nanyang Technological University, Singapore
5. Chinese Academy of Sciences, China
6. NTT Secure Platform Laboratories, Japan

FSE 2019, Paris, France @ March 25, 2019

Overview

1. **Background and Motivation**
2. **Preliminary**
3. **Overview of Our Attacks**
4. **Attacks on AES-PRF**
5. **Attacks on Dual-AES-PRF**
6. **Summary and Conclusion**

Background and Motivation

Background

Pseudorandom permutation (PRP)

- Main primitives in symmetric-key cryptography
- Ultimate security goal in the design of block ciphers
- Many secure block ciphers are readily available, e.g., AES

Background

Pseudorandom permutation (PRP)

- Main primitives in symmetric-key cryptography
- Ultimate security goal in the design of block ciphers
- Many secure block ciphers are readily available, e.g., AES

Pseudorandom function (PRF)

- Invertibility is unnecessary
- CTR encryption mode, authenticated encryption GCM

Background

Pseudorandom permutation (PRP)

- Main primitives in symmetric-key cryptography
- Ultimate security goal in the design of block ciphers
- Many secure block ciphers are readily available, e.g., AES

Pseudorandom function (PRF)

- Invertibility is unnecessary
- CTR encryption mode, authenticated encryption GCM

PRP-to-PRF conversion

- Large efficiency costs design, e.g., Truncation, XOR of Permutations (XoP), Encrypted Davies-Meyer (EDM), The Dual of EDM (EDMD)
- Dedicated design with small efficiency costs, e.g., FastPRF,

$$\mathrm{FastPRF}_K(X) = E_K(X) \oplus E_K^1(X).$$

Motivation

Observations

- $\text{AES-PRF}_{s,t}$ is as efficient as AES
- Efficiency and cost-effectiveness comes at the cost of provable security
- Provable security result of EDMD no longer applies to AES-PRF

Open Problems

- $(s, t) = (2, 8)$ is left as an open question
- The security of $\text{AES-PRF}_{s,t}$
- The security of the dual version (Dual-AES-PRF)

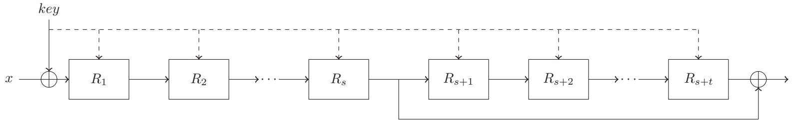
Methods

- ID, ZC, DC, and MITM

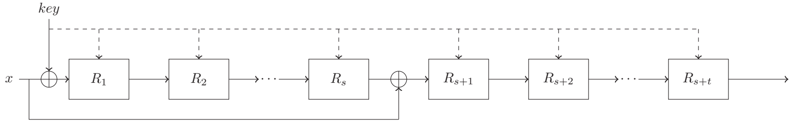
Preliminary

AES-PRF & Dual-AES-PRF

- AES-PRF$_{s,t}$ (Mennink and Neves @ FSE 2018)



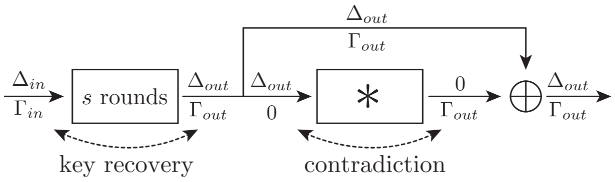
- Dual-AES-PRF$_{s,t}$



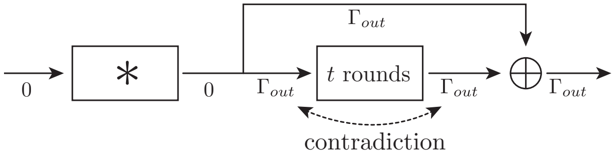
Overview of Our Attacks

Attacks on AES-PRF

Impossible differential/Zero-correlation attacks ($s \leqslant 2$)



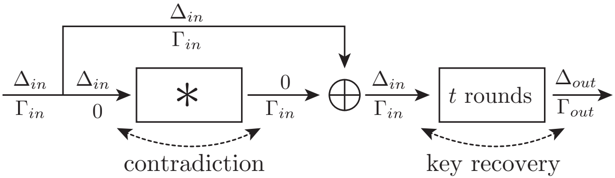
Zero-correlation distinguishers ($t \leqslant 4$)



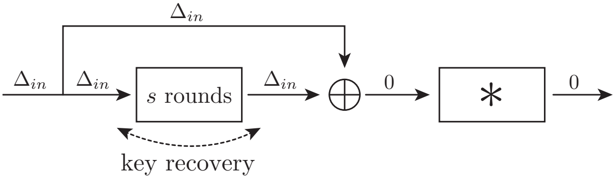
Meet-in-the-middle attacks on AES-PRF$_{s,7-s}$

Attacks on Dual-AES-PRF

Impossible differential/Zero-correlation attacks ($t \leqslant 2$)

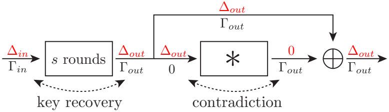


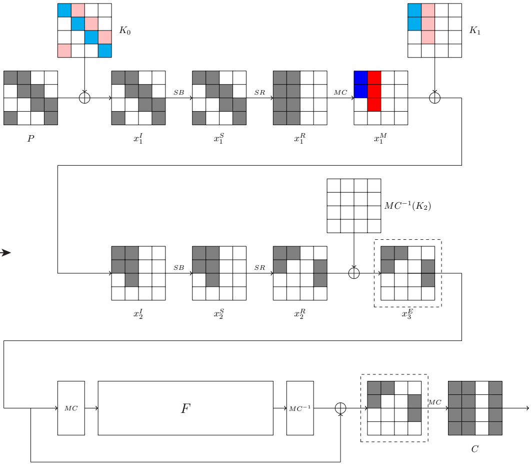
Differential attacks ($s \leqslant 4$)



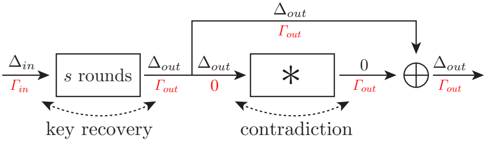
Attacks on AES-PRF

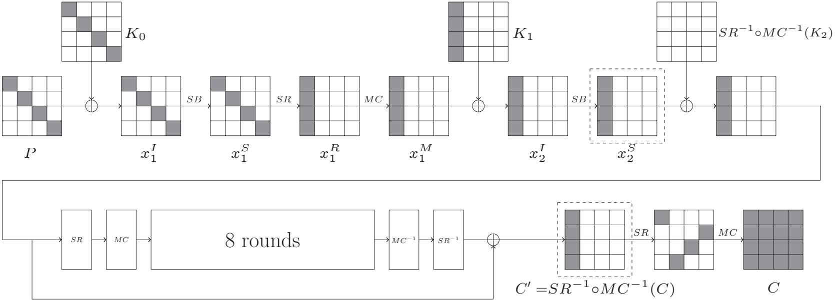
Impossible Differential Attack for AES-PRF$_{2,8}$



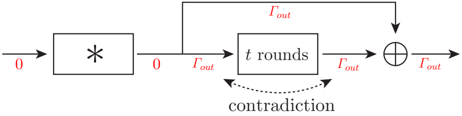


Zero-Correlation Linear Attack for AES-PRF$_{2,8}$

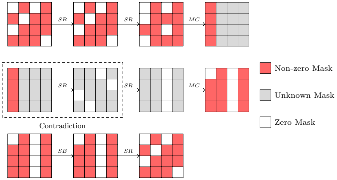




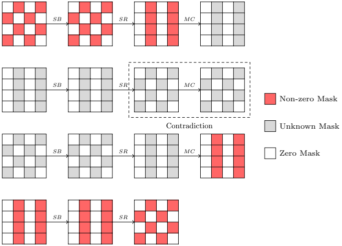
Distinguishers against AES-PRF$_{7,3}$ & AES-PRF$_{6,4}$



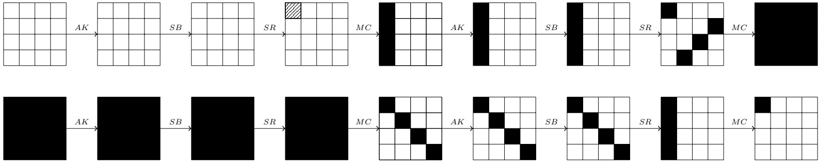
ZC Distinguisher for AES$_3$



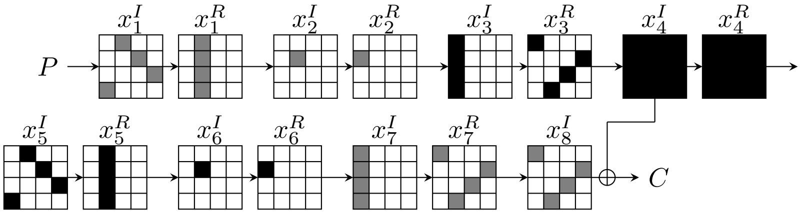
ZC Distinguisher for AES$_4$



Attack against AES-PRF$_{3,4}$

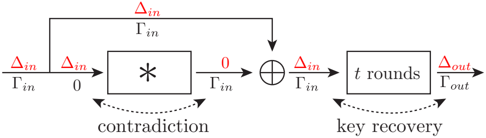


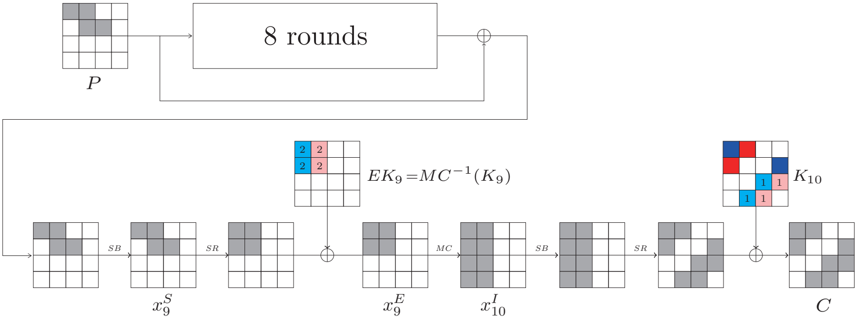
- The number of possible sequences: $(2^8)^{255} = 2^{2040} \longrightarrow (2^8)^{25} = 2^{200}$



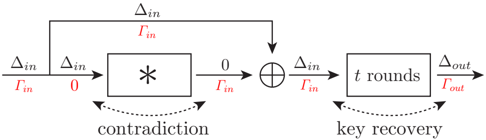
Attacks on Dual-AES-PRF

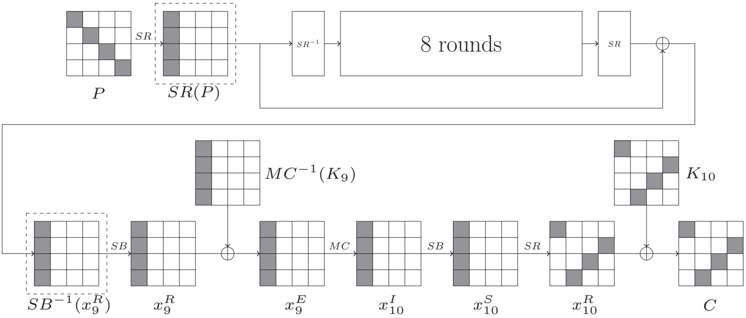
Impossible Differential Attack for Dual-AES-PRF$_{2,8}$



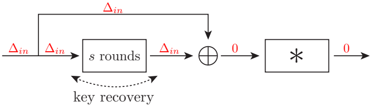


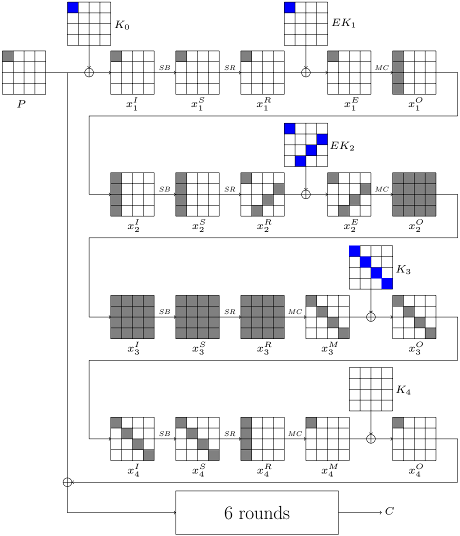
Zero-correlation attack for Dual-AES-PRF$_{8,2}$





Differential Attack for Dual-AES-PRF$_{4,6}$





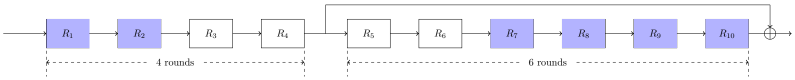
Summary and Conclusion

Summary

Target	s	t	Time	Data	Memory	Method	Ref
AES-PRF	1	*	2^{101}	2^{67} CP	2^{67}	ID	@FSE 2017
	*	1	–	–	–	Statistics	
AES-PRF	1	*	2^{71}	2^{71} CP	2^{64}	ID	Our Results
	1	*	$2^{122.49}$	$2^{103.34}$ KP	2^{96}	ZC	
	2	*	2^{94}	2^{94} CP	2^{88}	ID	
	2	*	$2^{115.14}$	$2^{115.06}$ KP	2^{65}	ZC	
	*	3	$2^{84.96}$	$2^{84.96}$ KP	$2^{84.96}$	ZC distinguisher	
	*	4	$2^{96.95}$	$2^{96.95}$ KP	2^{64}	ZC distinguisher	
	s	$7-s$	2^{107}	2^{107} CP	2^{104}	MitM	
Dual-AES-PRF	*	1	2^{71}	2^{71} CP	2^{64}	ID	Our Results
	*	1	$2^{122.49}$	$2^{103.34}$ KP	2^{96}	ZC	
	*	2	2^{104}	2^{104} CP	2^{72}	ID	
	*	2	$2^{115.14}$	$2^{115.06}$ KP	2^{65}	ZC	
	3	*	2^{97}	2^{97} CP	2^{32}	Differential	
	4	*	2^{121}	2^{121} CP	2^{8}	Differential	

Conclusion

- Comparison between AES-PRF and Dual-AES-PRF
  - The security of AES-PRF is **higher** than Dual-AES-PRF from the applicability of differential attacks.
  - Both AES-PRF and Dual-AES-PRF **have only one** round as the security margin.
- Choice of the parameter
  - The balanced case AES-PRF$_{5,5}$ is certainly a natural choice of the design.
  - However, our results indicate that $(s, t) = (4, 6)$ for AES-PRF is potential to be more secure, since the margin with respect to the attacked rounds becomes larger.



Thank you for your attention!

Thank the anonymous FSE 2019 reviewers and Samuel Neves for careful reading and many helpful comments.

Thank all the group members at ASK 2017 for the fruitful discussion.