Improved Rectangle Attacks on SKINNY and CRAFT

Hosein Hadipour Nasour Bagheri Ling Song

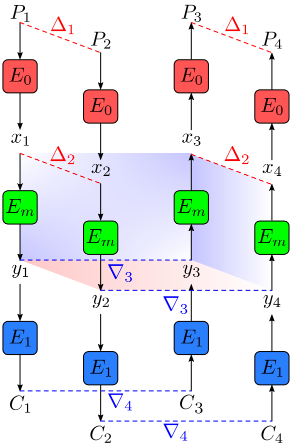
FSE 2022

SCIENCE
PASSION
TECHNOLOGY

Outline

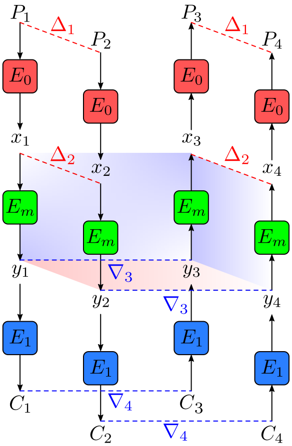
Sandwich Distinguishers

Sandwich Distinguisher [DKS10; DKS14]



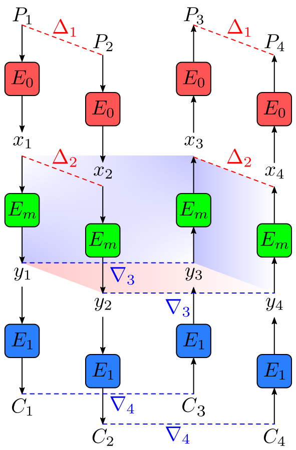
Hosein Hadipour, Nasour Bagheri, Ling Song

Sandwich Distinguisher [DKS10; DKS14]



$$\Pr(\Delta_1 \xrightarrow{E_0} \Delta_2) = p;$$

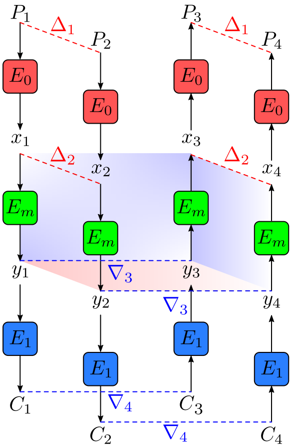
Sandwich Distinguisher [DKS10; DKS14]



$$\Pr(\Delta_1 \xrightarrow{E_0} \Delta_2) = p; \quad \Pr(\nabla_3 \xrightarrow{E_1} \nabla_4) = q$$

Hosein Hadipour, Nasour Bagheri, Ling Song

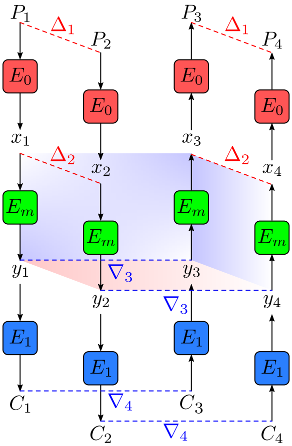
Sandwich Distinguisher [DKS10; DKS14]



$$\Pr(P_3 \oplus P_4 = \Delta_1) \approx p^2 \times r \times q^2$$

Hosein Hadipour, Nasour Bagheri, Ling Song

Sandwich Distinguisher [DKS10; DKS14]



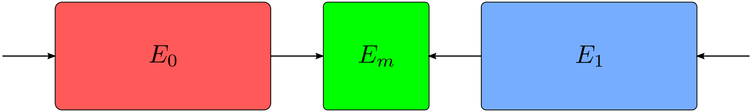
$$\Pr(P_3 \oplus P_4 = \Delta_1) \approx p^2 \times r \times q^2$$

$$r = r(\Delta_2, \nabla_3) = \Pr\{E_m^{-1}(E_m(x) \oplus \nabla_3) \oplus E_m^{-1}(E_m(x \oplus \Delta_2) \oplus \nabla_3) = \Delta_2\}$$

Hosein Hadipour, Nasour Bagheri, Ling Song

Effective Parameters in p^2q^2r for SPN Ciphers

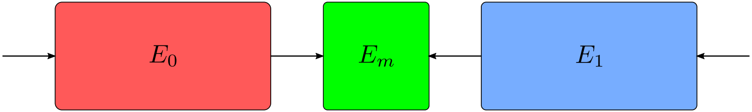
- p is mostly determined by the number of active S-boxes in E_0
- q is mostly determined by the number of active S-boxes in E_1
- r is mostly determined by the number of common active S-boxes in E_m
- Active S-boxes in E_0, E_1 are more expensive than common active S-boxes in E_m



Hosein Hadipour, Nasour Bagheri, Ling Song

Effective Parameters in p^2q^2r for SPN Ciphers

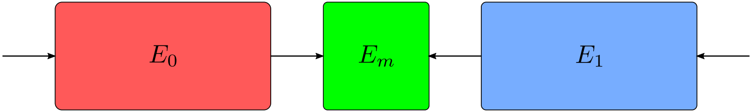
- p is mostly determined by the number of active S-boxes in E_0
- q is mostly determined by the number of active S-boxes in E_1
- r is mostly determined by the number of common active S-boxes in E_m
- Active S-boxes in E_0, E_1 are more expensive than common active S-boxes in E_m



Hosein Hadipour, Nasour Bagheri, Ling Song

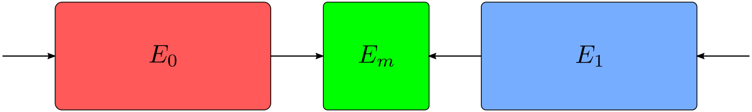
Effective Parameters in p^2q^2r for SPN Ciphers

- p is mostly determined by the number of active S-boxes in E_0
- q is mostly determined by the number of active S-boxes in E_1
- r is mostly determined by the number of common active S-boxes in E_m
- Active S-boxes in E_0, E_1 are more expensive than common active S-boxes in E_m



Effective Parameters in p^2q^2r for SPN Ciphers

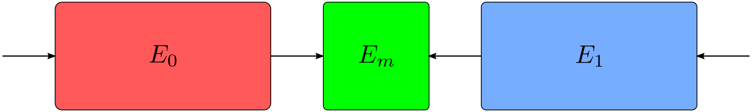
- p is mostly determined by the number of active S-boxes in E_0
- q is mostly determined by the number of active S-boxes in E_1
- r is mostly determined by the number of common active S-boxes in E_m
- Active S-boxes in E_0, E_1 are more expensive than common active S-boxes in E_m



Hosein Hadipour, Nasour Bagheri, Ling Song

Effective Parameters in p^2q^2r for SPN Ciphers

- p is mostly determined by the number of active S-boxes in E_0
- q is mostly determined by the number of active S-boxes in E_1
- r is mostly determined by the number of common active S-boxes in E_m
- Active S-boxes in E_0, E_1 are more expensive than common active S-boxes in E_m



Our Method To Find Sandwich Distinguishers

Our Method to Find Sandwich Distinguishers

Our method consists of 3 main steps:

- Find the truncated upper and lower trails minimizing:
  - number of active S-boxes in outer parts
  - and number of common active S-boxes in the middle part
- Instantiate the discovered truncated trails with concrete differential trails
- Compute p, q and r to derive the entire probability, i.e., p^2q^2r

Our Method to Find Sandwich Distinguishers

Our method consists of 3 main steps:

- Find the truncated upper and lower trails minimizing:
  - number of active S-boxes in outer parts
  - and number of common active S-boxes in the middle part
- Instantiate the discovered truncated trails with concrete differential trails
- Compute p, q and r to derive the entire probability, i.e., p^2q^2r

Our Method to Find Sandwich Distinguishers

Our method consists of 3 main steps:

- Find the truncated upper and lower trails minimizing:
  - number of active S-boxes in outer parts
  - and number of common active S-boxes in the middle part
- Instantiate the discovered truncated trails with concrete differential trails
- Compute p, q and r to derive the entire probability, i.e., p^2q^2r

Hosein Hadipour, Nasour Bagheri, Ling Song

Our Method to Find Sandwich Distinguishers

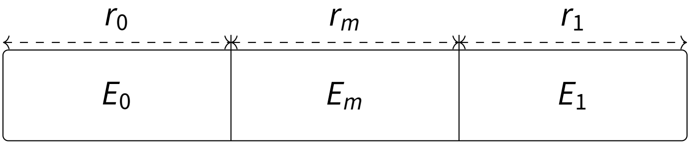
Our method consists of 3 main steps:

- Find the truncated upper and lower trails minimizing:
  - number of active S-boxes in outer parts
  - and number of common active S-boxes in the middle part
- Instantiate the discovered truncated trails with concrete differential trails
- Compute p, q and r to derive the entire probability, i.e., p^2q^2r

Finding Appropriate Truncated Upper and Lower Trails

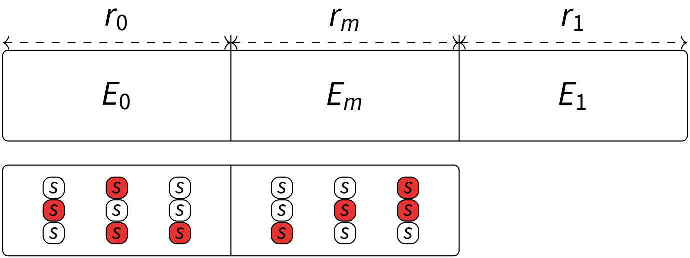
$$\boxed{\quad E \quad}$$

Finding Appropriate Truncated Upper and Lower Trails

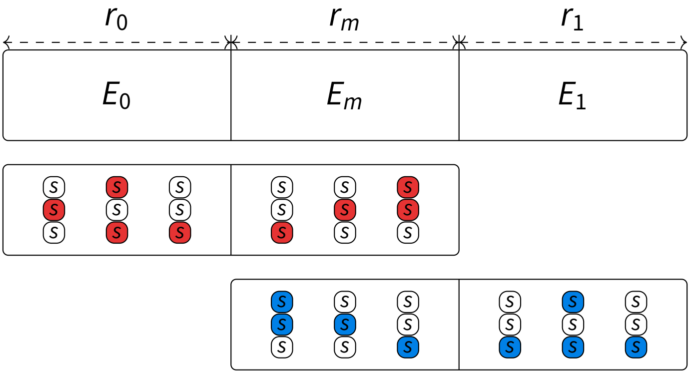


Hosein Hadipour, Nasour Bagheri, Ling Song

Finding Appropriate Truncated Upper and Lower Trails

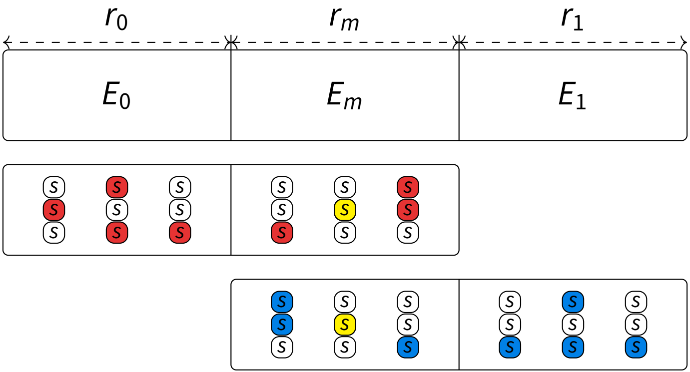


Finding Appropriate Truncated Upper and Lower Trails



Hosein Hadipour, Nasour Bagheri, Ling Song

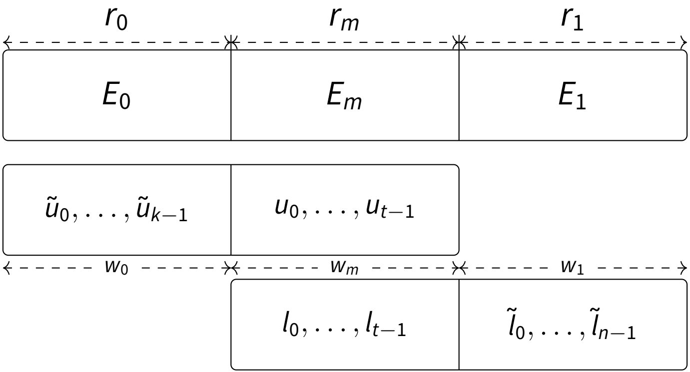
Finding Appropriate Truncated Upper and Lower Trails



$$u_i - s_i \geq 0, \ \ell_i - s_i \geq 0, \ -u_i - \ell_i + s_i \geq -1$$

Hosein Hadipour, Nasour Bagheri, Ling Song

Finding Appropriate Truncated Upper and Lower Trails



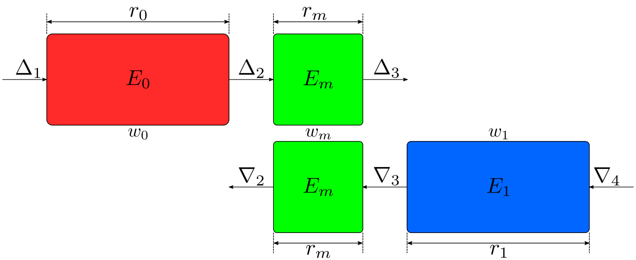
$$\min \sum_{i=0}^{k-1} w_0 \cdot \tilde{u}_i + \sum_{j=0}^{t-1} w_m \cdot s_j + \sum_{k=0}^{n-1} w_1 \cdot \tilde{l}_k.$$

$$u_i - s_i \geq 0, \;\; \ell_i - s_i \geq 0, \;\; -u_i - \ell_i + s_i \geq -1.$$

Hosein Hadipour, Nasour Bagheri, Ling Song

Instantiating Truncated Trails with Concrete Differentials

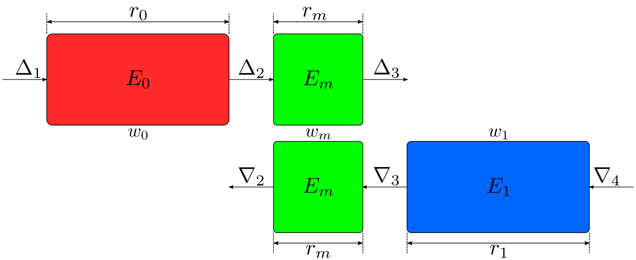
- We Instantiate the first and last parts with concrete bit-wise differentials
- **Our distinguishers are not relied on differential characteristics for** E_0, E_1, E_m
- To compute p, q and r we fix the differences at only four positions



Hosein Hadipour, Nasour Bagheri, Ling Song

Instantiating Truncated Trails with Concrete Differentials

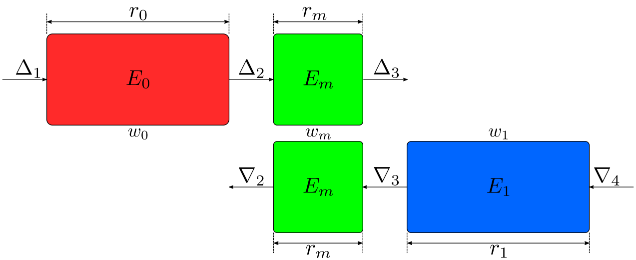
- We Instantiate the first and last parts with concrete bit-wise differentials
- Our distinguishers are not relied on differential characteristics for E_0, E_1, E_m
- To compute p, q and r we fix the differences at only four positions



Hosein Hadipour, Nasour Bagheri, Ling Song

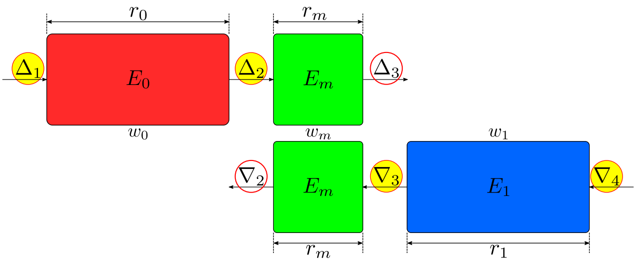
Instantiating Truncated Trails with Concrete Differentials

- We Instantiate the first and last parts with concrete bit-wise differentials
- **Our distinguishers are not relied on differential characteristics for** E_0, E_1, E_m
- To compute p, q and r we fix the differences at only four positions



Instantiating Truncated Trails with Concrete Differentials

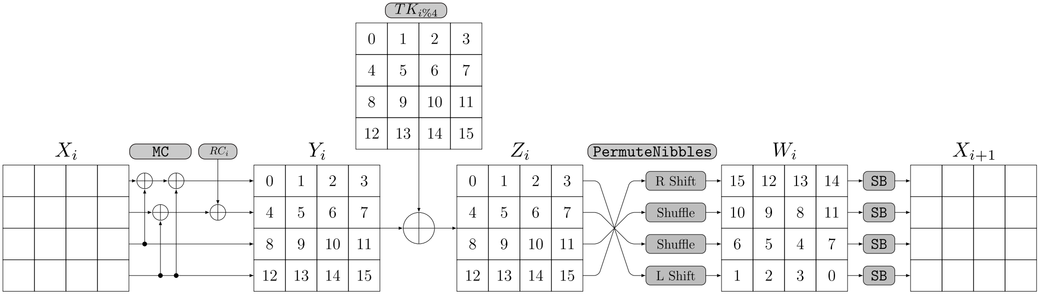
- We Instantiate the first and last parts with concrete bit-wise differentials
- **Our distinguishers are not relied on differential characteristics for** E_0, E_1, E_m
- To compute p, q and r we fix the differences at only four positions



Hosein Hadipour, Nasour Bagheri, Ling Song

Application to CRAFT

CRAFT [Bei+19]



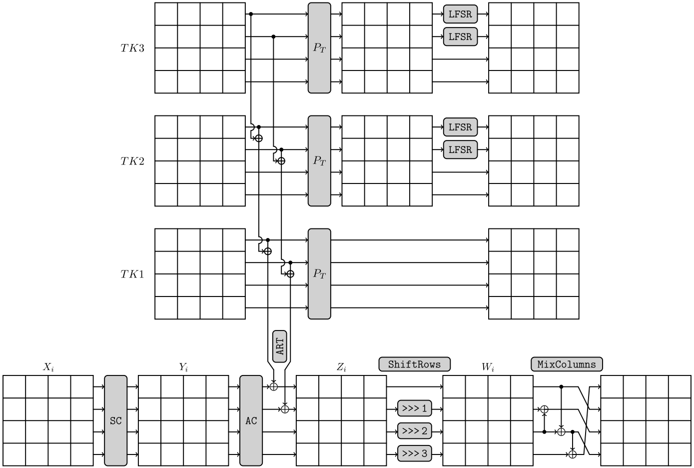
Hosein Hadipour, Nasour Bagheri, Ling Song

Summary of Our Distinguishers for CRAFT

Distinguisher Type	# Rounds	Probability	Reference
ST-Differential	9	$2^{-40.20}$	[Had+19]
	10	$2^{-44.89}$	
	11	$2^{-49.79}$	
	12	$2^{-54.48}$	
	13	$2^{-59.13}$	
	14	$2^{-63.80}$	
ST-Boomerang	6	$\mathbf{1}$	This Paper
	7	$\mathbf{2^{-4}}$	
	8	$\mathbf{2^{-8}}$	
	9	$\mathbf{2^{-14.76}}$	
	10	$\mathbf{2^{-19.83}}$	
	11	$\mathbf{2^{-24.90}}$	
	12	$\mathbf{2^{-34.89}}$	
	13	$2^{-44.89}$	
	14	$2^{-55.85}$	

Application to SKINNY

SKINNY [Bei+16]



Summary of Our Distinguishers for SKINNY

Version	n	#Rounds	Probability: Our Distinguisher	Probability: [SQH19]
SKINNY-n-$2n$	64	17	$\mathbf{2^{-26.54}}$(II)	$2^{-29.78}$
		18	$\mathbf{2^{-37.90}}$(II)	$2^{-45.14}$
		19	$\mathbf{2^{-51.08}}$(II)	$2^{-65.62}$
	128	18	$\mathbf{2^{-40.77}}$ (II)	$2^{-77.83}$
		19	$\mathbf{2^{-58.33}}$ (II)	$2^{-97.53}$
		20	$\mathbf{2^{-85.31}}$ (I)	$2^{-128.65}$
		21	$\mathbf{2^{-114.07}}$ (II)	$2^{-171.77}$
SKINNY-n-$3n$	64	22	$\mathbf{2^{-38.84}}$ (I)	$2^{-42.98}$
		23	$\mathbf{2^{-52.84}}$ (I)	$2^{-67.36}$
	128	22	$\mathbf{2^{-40.57}}$ (I)	$2^{-48.30}$
		23	$\mathbf{2^{-56.47}}$ (I)	$2^{-75.86}$
		24	$\mathbf{2^{-87.39}}$ (I)	$2^{-107.86}$
		25	$\mathbf{2^{-116.59}}$ (I)	$2^{-141.66}$

Summary of Our Key Recovery Attacks

Scheme	#rounds	Data	Memory	Time	Attack	P_s	Reference
SKINNY-64-128	23/36	$2^{60.54}$	$2^{60.9}$	$2^{120.7}$	Rectangle	0.977	This paper
SKINNY-64-192	29/40	$2^{61.42}$	2^{80}	2^{178}	Rectangle	0.977	This paper
SKINNY-128-256	24/48	$2^{125.21}$	$2^{125.54}$	$2^{209.85}$	Rectangle	0.977	This paper
SKINNY-128-384	30/56	$2^{125.29}$	$2^{125.8}$	$2^{361.68}$	Rectangle	0.977	This paper
CRAFT	18/32	$2^{60.92}$	2^{84}	$2^{101.7}$	Rectangle	0.977	This paper
SKINNY-64-128	23/36	$2^{62.47}$	2^{124}	$2^{125.91}$	Impossible	1	[LGS17]
SKINNY-64-192	27/40	$2^{63.5}$	2^{80}	$2^{165.5}$	Rectangle	0.916	[LGS17]
SKINNY-128-256	23/48	$2^{124.47}$	2^{248}	$2^{251.47}$	Impossible	1	[LGS17]
SKINNY-128-384	28/56	2^{122}	$2^{122.32}$	$2^{315.25}$	Rectangle	0.8315	[Zha+20]

Hosein Hadipour, Nasour Bagheri, Ling Song

Conclusion

Our Main Contributions

- We introduced a heuristic method to search for sandwich distinguishers
- We introduced new tools in BCT framework (`DBCT`, ...)
- We significantly improved the rectangle attacks on SKINNY and CRAFT

Thanks for your attention!

https://github.com/hadipourh/Boomerang

Hosein Hadipour, Nasour Bagheri, Ling Song

Bibliography I

[Bei+16] Christof Beierle et al. **The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS.** CRYPTO (2). Vol. 9815. Lecture Notes in Computer Science. Springer, 2016, pp. 123–153.

[Bei+19] Christof Beierle et al. **CRAFT: Lightweight Tweakable Block Cipher with Efficient Protection Against DFA Attacks.** *IACR Trans. Symmetric Cryptol.* 2019.1 (2019), pp. 5–45.

[DKS10] Orr Dunkelman, Nathan Keller, and Adi Shamir. **A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony.** CRYPTO. Vol. 6223. Lecture Notes in Computer Science. Springer, 2010, pp. 393–410.

[DKS14] Orr Dunkelman, Nathan Keller, and Adi Shamir. **A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony.** *J. Cryptol.* 27.4 (2014), pp. 824–849.

[Had+19] Hosein Hadipour et al. **Comprehensive security analysis of CRAFT.** *IACR Trans. Symmetric Cryptol.* 2019.4 (2019), pp. 290–317.

Bibliography II

[LGS17] Guozhen Liu, Mohona Ghosh, and Ling Song. **Security Analysis of SKINNY under Related-Tweakey Settings.** *IACR Transactions on Symmetric Cryptology* 2017.3 (Sept. 2017). https://tosc.iacr.org/index.php/ToSC/article/view/765, pp. 37–72. DOI: 10.13154/tosc.v2017.i3.37-72.

[SQH19] Ling Song, Xianrui Qin, and Lei Hu. **Boomerang Connectivity Table Revisited. Application to SKINNY and AES.** *IACR Trans. Symmetric Cryptol.* 2019.1 (2019), pp. 118–141.

[Zha+20] Boxin Zhao et al. **Generalized related-key rectangle attacks on block ciphers with linear key schedule: applications to SKINNY and GIFT.** *Designs, Codes and Cryptography* 88.6 (2020), pp. 1103–1126.