Cryptanalysis of Full SCARF

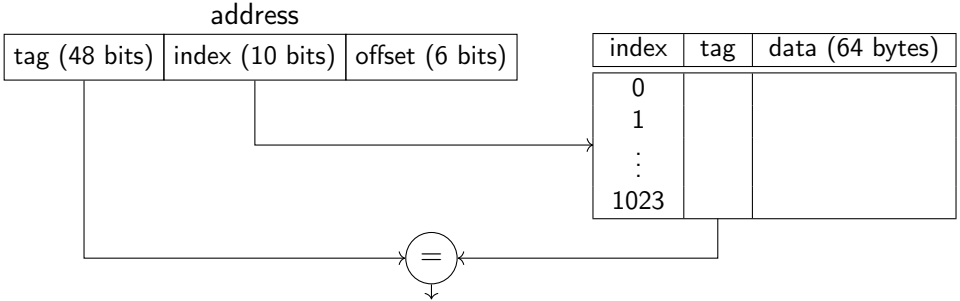
Antonio Flórez-Gutiérrez Eran Lambooij Gaëtan Leurent Håvard Raddum
Tyge Tiessen **Michiel Verbauwhede**

Eurocrypt 2025

COSIC

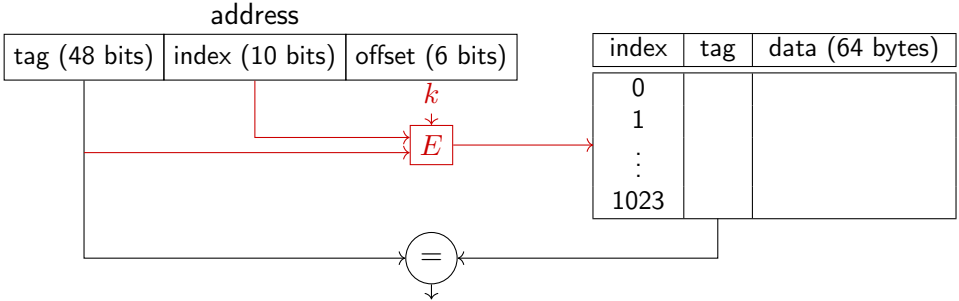
KU LEUVEN

Tweakable Block Cipher for Cache Randomization



- Side-channel information from collision between indices

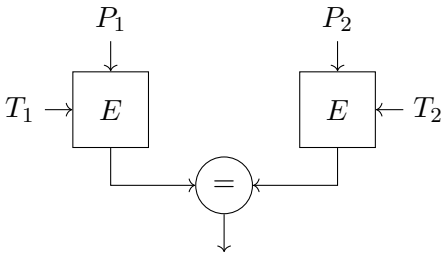
Tweakable Block Cipher for Cache Randomization



- Side-channel information from collision between indices
- Add tweakable block cipher to randomize indices: Scattercache [Werner et al., 2019]
- SCARF: 10 bit block cipher with 48 bit tweak and 240 bit key [Canale et al., 2023]

Attacker Model

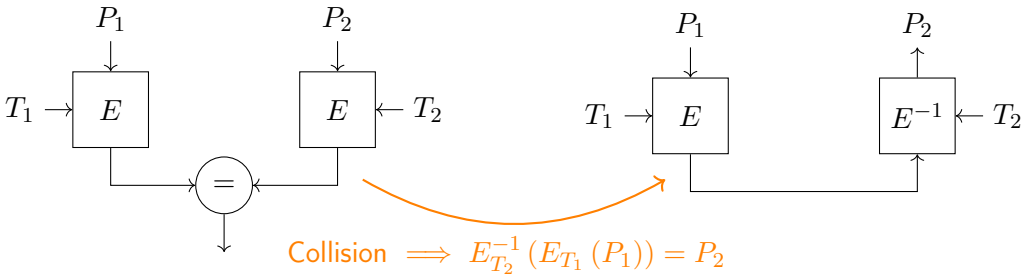
Collision Model



Attacker Model

Collision Model

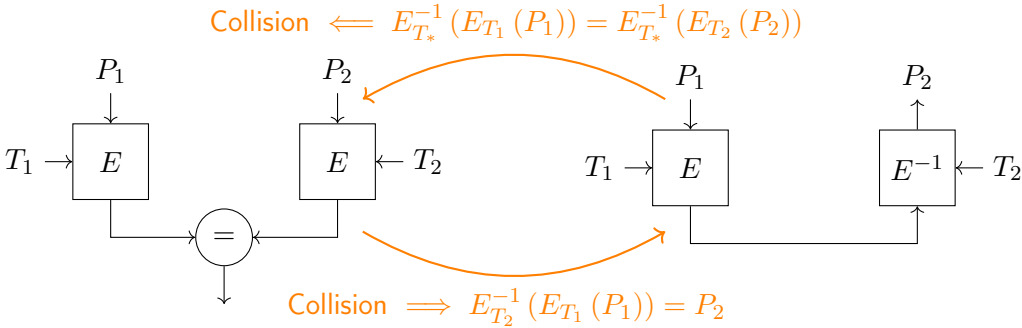
Encryption-Decryption Model



Attacker Model

Collision Model

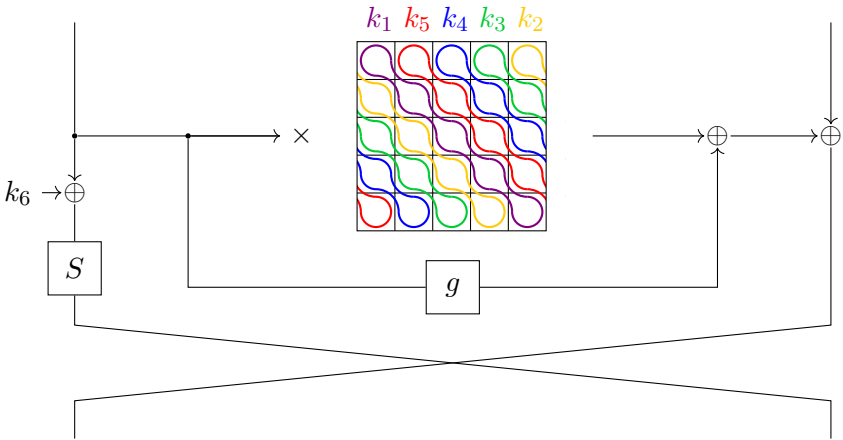
Encryption-Decryption Model



- Distinguish either model in 2^{40} data and 2^{80} time

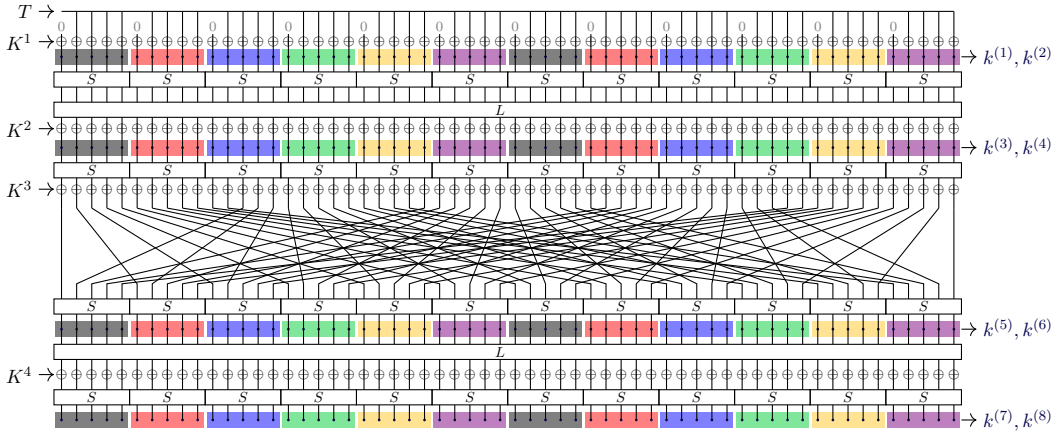
SCARF

Round Function



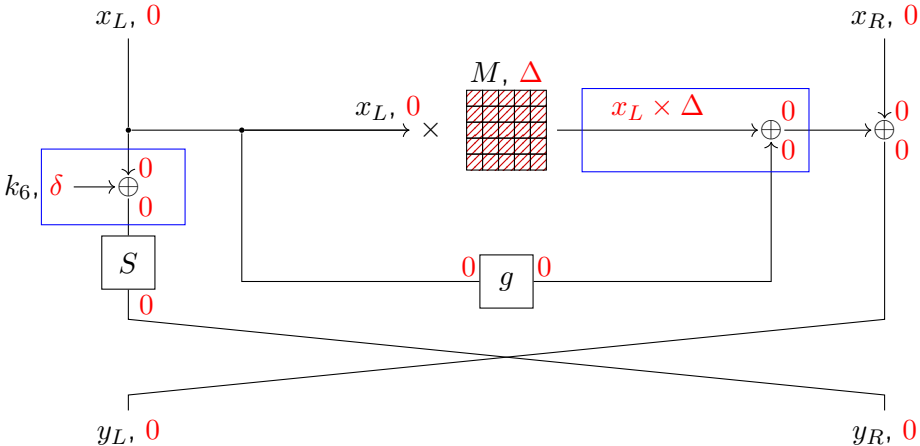
SCARF

Tweakey Schedule



Distinguisher in the Collision Model

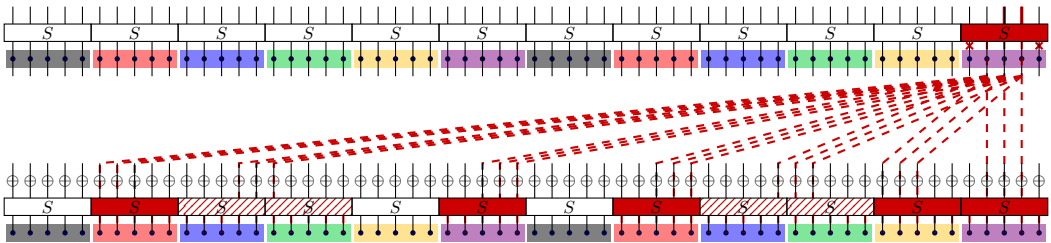
Collisions in the Round Function



- Collision over 1 round if $\delta = 0$ and $x_L \in \ker(\Delta)$

Distinguisher in the Collision Model

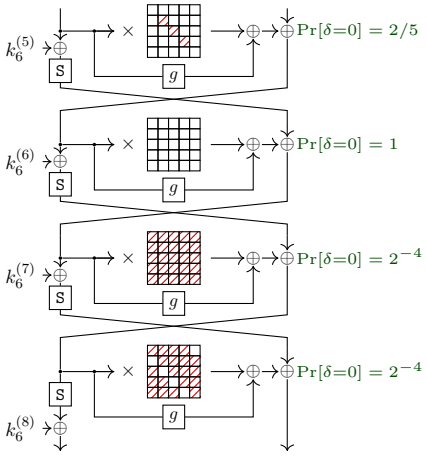
Truncated Differential in the Tweakey Schedule



- Probability of transition through first SBox layer: $5/16$

Distinguisher in the Collision Model

Full Data Path Collision



4-Round Distinguisher

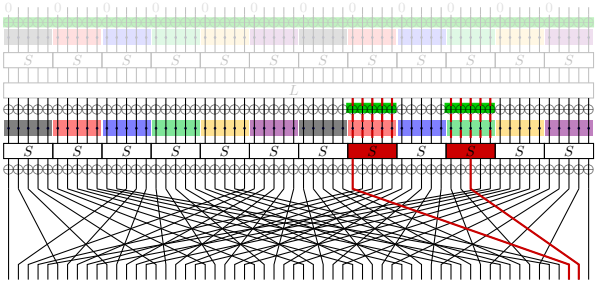
- Tweakey schedule: 5×2^{-4}
- Data path: $2^{-7}/5$
- Estimated probability of collision: $2^{-10} + 2^{-11}$
- Observed probability of collision: $2^{-10} + 2^{-10.5}$

6-Round Distinguisher

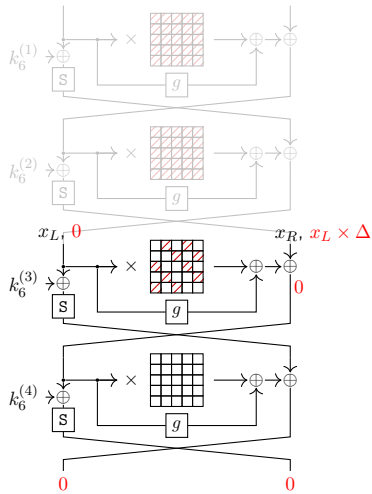
- Probability of collision: $2^{-10} + 2^{-17.8}$
- Data Complexity: 2^{30}

Key Recovery

Simple Idea



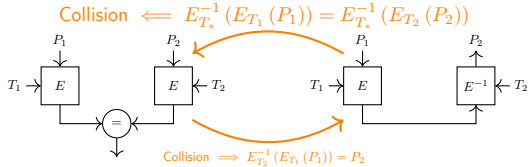
- Guess K^1 and solve for collisions on the first 4 rounds of the data path
- Guess additional 10 bits to solve for the correct input difference to distinguisher
- Problem: How can we reuse data between key guesses?



Key Recovery

Reducing Data Complexity

Simulate Collision Model with Encryption-Decryption Model



- All collision queries $E_{T_i}(P_i) = E_{T_j}(P_j)$ for $(T_i, P_i), (T_j, P_j) \in \mathcal{S}$ can be evaluated with $|\mathcal{S}|$ encryption-decryption queries

Choosing the Input Set $\mathcal{S}$

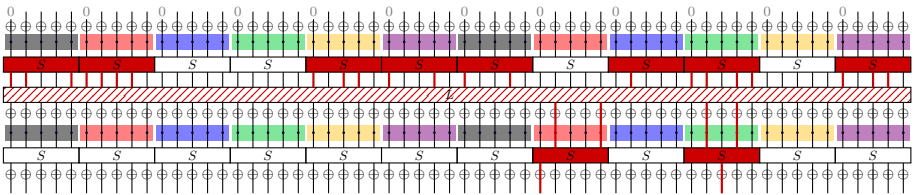
- $\mathcal{S} = \mathcal{T} \times \mathcal{P}$
- $\mathcal{P} = \mathbb{F}_2^{10}$, this guarantees 2^{10} right-pairs in the data path

Key Recovery

Reducing Data Complexity 2: Find Good Tweak Set

Choosing $\mathcal{S}$ (Continued)

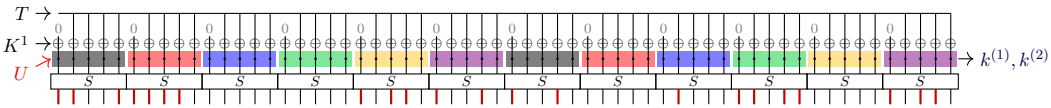
- Split $\mathcal{T}$ at Sbox boundaries: $\mathcal{T} = \mathcal{T}_1 \times \mathcal{T}_2 \times \cdots \times \mathcal{T}_{12}$
- Extend characteristic to minimize number of active Sboxes in first layer:



- Optimization Problem: find $\max_{\mathcal{T}} \left(\min_{K^1} \#\text{right pairs} \right)$
- Check minimum number of right pairs over K^2 with quasidifferential trails
- Result: 34 bits of filtering for 2^{39} data
- Problem: Naive time complexity is 2^{89}

Key Recovery

Reducing Time Complexity



1. Guess $\mathcal{U} = K^1 + \mathcal{T}$
2. Solve for all $(U, U') \in \mathcal{U}^2$ that satisfy the characteristic and corresponding (P, P') that collide after 4 rounds
3. Find all (T, T') that collide for (P, P') and satisfy $U + U' = T + T'$
4. Solve for K^1 and 10 bits of K^2

- Additional precomputed lookup tables
- Total complexity: 2^{77} time and 2^{39} data

Conclusion

Rounds	Model	Queries	Time	Note	Reference
4	enc-dec	2^{10}	2^{61}	Key recovery	[Chen et al., 2024]
7	enc-dec	2^{40}	2^{76}	Key recovery	[Boura et al., 2024]
8	enc-dec	2^{63}	2^{68}	Multikey distinguisher	[Boura et al., 2024]
6	collision	2^{30}	2^{30}	Distinguisher	this work
8	enc-dec	2^{39}	2^{77}	Key recovery	this work


Boura, C., Rasoolzadeh, S., Saha, D., and Todo, Y. (2024).
Multiple-tweak differential attack against SCARF.
In *ASIACRYPT 2024, Part VII*, LNCS, pages 330–360. Springer, Singapore.


Canale, F., Güneysu, T., Leander, G., Thoma, J. P., Todo, Y., and Ueno, R. (2023).
SCARF - A low-latency block cipher for secure cache-randomization.
In Calandrino, J. A. and Troncoso, C., editors, *USENIX Security 2023*, pages 1937–1954. USENIX Association.


Chen, S., Hu, K., Liu, G., Niu, Z., Tan, Q. Q., and Wang, S. (2024).
Meet-in-the-middle attack on 4+4 rounds of SCARF under single-tweak setting.
Cryptology ePrint Archive, Report 2024/1270.


Werner, M., Unterluggauer, T., Giner, L., Schwarz, M., Gruss, D., and Mangard, S. (2019).
Scattercache: Thwarting cache attacks via cache set randomization.
In Heninger, N. and Traynor, P., editors, *28th USENIX Security Symposium, USENIX Security 2019, Santa Clara, CA, USA, August 14-16, 2019*, pages 675–692. USENIX Association.