Symmetric Cryptanalysis – Submission Guidelines

- Timeline: Release **07. 05. 2020**; Question time **04. 06. 2020**; Submission **12. 06. 2020**
- Upload and tick your team's submissions on `https://stics.iaik.tugraz.at/`.
- Submit your code as a {`zip`, `tar.gz`} archive. Add a file `README.`{`md`, `txt`, `pdf`} on the top level that documents your submission (design, howto, limitations, runtime, references).
- You can use your favourite programming language, libraries, and existing open-source implementations of the target ciphers. Please document your choices in the `README`.
- *Hint:* For testing purposes, you can always assume that part of the key is already known to speed up the key recovery; e.g., if you're testing candidates for your 32-bit subkey, you can fix 16 bits to the correct value and only loop the remaining 16 bits.

2–A Related-Key Differential Analysis of AES (4 Points)

Analyze the differential properties of the AES block cipher [DR06] using MILP [Mou+11].

(a) 2-Round Differentials (2 Points): Find optimal 2-round differential characteristics for AES with expected probability 2^{-30} (use patterns with a single active column after round 1 and use the best transitions from the DDT). Perform a precise practical evaluation for a few keys (by exhaustively testing all values of this column). What do you observe?

(b) Related-Key Bounds (2 Points): Extend the MILP model from the lecture with the AES key schedule to derive bounds for the number of active S-boxes in related-key differential characteristics, where input differences are allowed in both plaintext and key.

[DR06] J. Daemen and V. Rijmen. "Understanding Two-Round Differentials in AES". In: *SCN 2006*. Vol. 4116. LNCS. `https://ia.cr/2006/039`. Springer, 2006, pp. 78–94. DOI: `10.1007/11832072_6`.

[Mou+11] N. Mouha, Q. Wang, D. Gu, and B. Preneel. "Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming". In: *Inscrypt 2011*. Vol. 7537. LNCS. Springer, 2011, pp. 57–76. DOI: `10.1007/978-3-642-34704-7_5`.

2–B Linear Cryptanalysis of PRESENT (8 Points)

Demonstrate linear cryptanalysis for PRESENT using the designers' considerations [Bog+07]. Choose a suitable linear approximation to recover (parts of) the secret key K.

(a) Find Approximation (3 Points): Compute the linear approximation table for the PRESENT S-boxes. Use it to find a good linear approximation for 9 rounds (Figure 1). Use a pattern similar to the lecture and try to find several compatible characteristics.

(b) Compute and Verify Bias (2 Points): Estimate the bias of your approximation. Experimentally verify it by testing it for a suitable number of plaintext-ciphertext pairs.

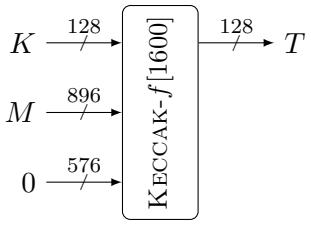
(c) 10-Round Attack (3 Points): Use the 9-round linear approximation for to recover parts of the secret key for PRESENT reduced to 10 rounds with Matsui's Algorithm 2.

[Bog+07] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe. "PRESENT: An Ultra-Lightweight Block Cipher". In: *CHES 2007*. Ed. by P. Paillier and I. Verbauwhede. Vol. 4727. LNCS. Springer, 2007, pp. 450–466. DOI: 10.1007/978-3-540-74735-2_31.

[Mat93] M. Matsui. "Linear Cryptanalysis Method for DES Cipher". In: *EUROCRYPT 1993*. Vol. 765. LNCS. Springer, 1993, pp. 386–397. DOI: 10.1007/3-540-48285-7_33.

2–C Cube Attack on Keccak-MAC (12 Points)

Demonstrate the cube attack to recover the key of a KECCAK-based MAC for short messages, similar to Dinur et al. [Din+15]. The MAC maps a 128-bit key K and message M of 896 bits (after padding) to a 128-bit authentication tag $T = h(K\|M\|0)$, where h is the KECCAK-f[1600] permutation with output truncated to 128 bits.



Target short messages, ignore the padding (see figure). Reduce the KECCAK-f[1600] permutation to 4 rounds (d) or fewer (a–c):

(a) Cube Sum (3 Points): Write a function to compute the cube sum (higher-order differential) for the round-reduced MAC by summing the tags T for a fixed key K and all elements of the specified cube for M (cube bits loop, the rest of the message is fixed). Verify the zero-sum property for a suitable cube size.

(b) Offline Phase (3 Points): Implement the offline phase of the cube attack: Pick a cube candidate and test (for each output bit) if the superpoly is linear by comparing the cube sum for suitable chosen key candidates. If the test fails, adapt the cube candidate; if it succeeds (for some output bits), store the cube candidate and the superpoly coefficients found by choosing suitable keys.

(c) Online Phase (3 Points): Implement the online phase of the cube attack: For each cube candidate identified in the offline phase, evaluate the cube for the target key and store the resulting equation. Find sufficiently many equations and solve the system.

(d) 4-Round Attack (3 Points): Apply your ingredients to recover (most of) the key for the MAC reduced to 4 rounds of KECCAK-f[1600].

[Din+15] I. Dinur, P. Morawiecki, J. Pieprzyk, M. Srebrny, and M. Straus. "Cube Attacks and Cube-Attack-Like Cryptanalysis on the Round-Reduced Keccak Sponge Function". In: *EUROCRYPT 2015*. Vol. 9056. LNCS. Springer, 2015, pp. 733–761. DOI: 10.1007/978-3-662-46800-5_28. URL: http://ia.cr/2014/736.

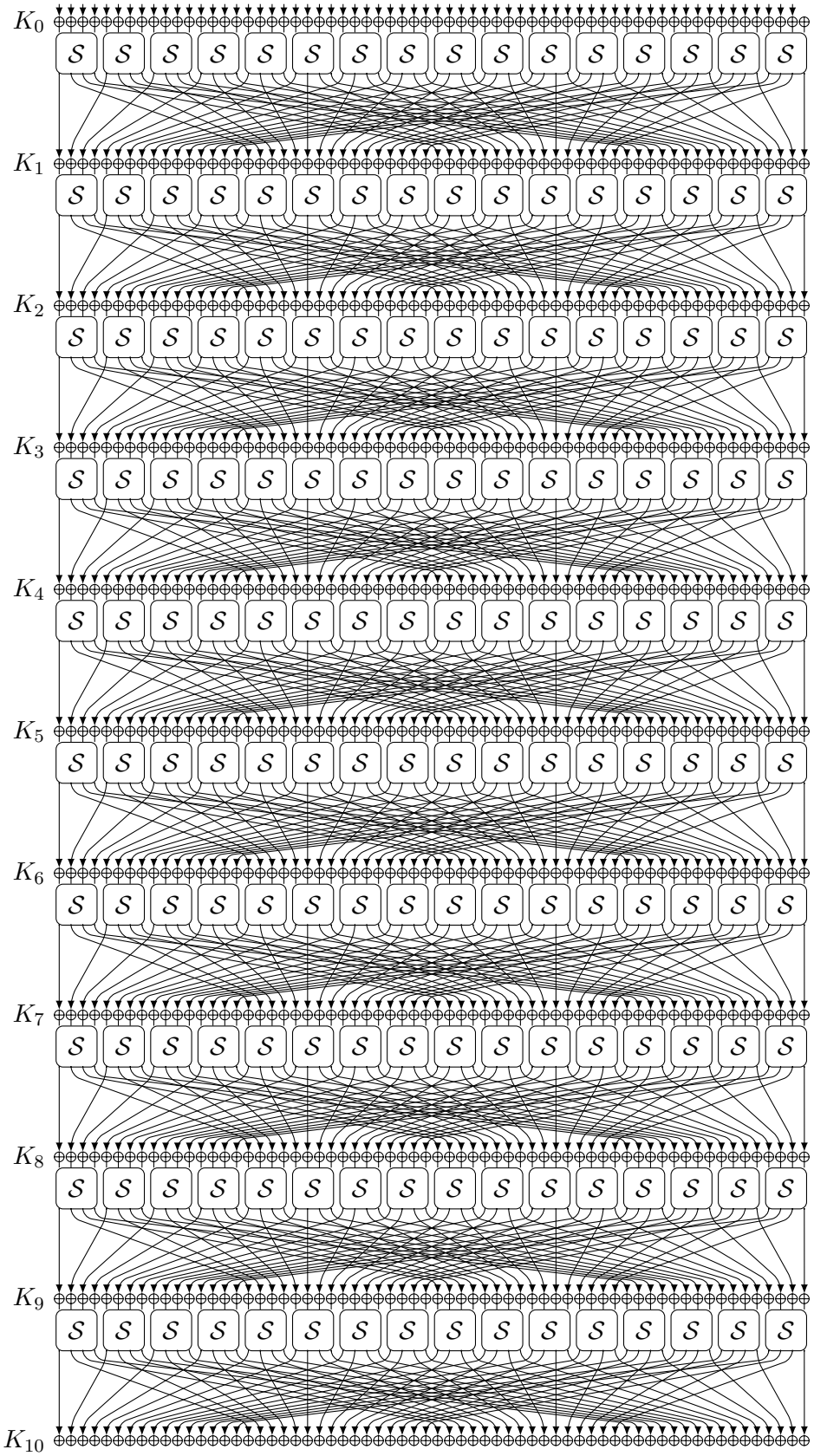


Fig. 1: Linear characteristic for 9-round PRESENT.