Symmetric Cryptanalysis – Submission Guidelines

- Timeline: Release **17. 03. 2016**; Question time **14. 04. 2016**; Submission **05. 05. 2016**
- Upload your team's submission on `https://stics.iaik.tugraz.at/`. Each task is uploaded separately. Don't forget to tick the selected tasks!
- You can use your favourite programming language – please document how to compile and use your implementations in `README.{txt,pdf,md}`.
- You can use any existing open-source implementations of the target ciphers. Include a clear and unambiguous reference in the `README`, and include the reference source so that we can compile your submission without downloading any additional non-standard libraries.
- For testing purposes, you can always assume that part of the key is already known to speed up the key recovery; i.e., 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.

1–A Linear Cryptanalysis of DES (4 Points)

Demonstrate linear cryptanalysis for DES, similar to Matsui [Mat93]. Choose a suitable linear approximation to recover (parts of) the secret key K. *Hint:* You may omit the initial and final permutation IP and IP^{-1} of DES to simplify the implementation of the attack.

(a) Linear Approximations (2 Points): Experimentally verify the bias of the linear approximations of Matsui for 3, 5, and 7 rounds of DES.

(b) 8-Round Attack (2 Points): Use the linear approximation for 7 rounds of DES to recover parts of the secret key for DES reduced to 8 rounds.

[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.

1–B Square Attack on AES (8 Points)

Demonstrate the Square attack for round-reduced AES, similar to Daemen, Knudsen, and Rijmen [DKR97] for the block cipher Square. Choose a suitable Λ-set to recover the secret key K for AES reduced to 4 and 5 rounds.

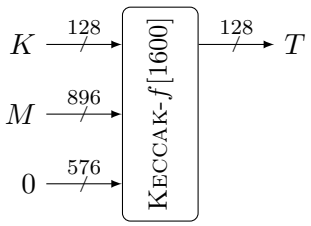
(a) 4 Rounds (4 Points): Verify the distinguishing property for 3 rounds of AES and show how this can be used to efficiently recover the secret key K for 4 rounds of AES.

(b) 5 Rounds (4 Points): Show how the attack on 4 rounds of AES can be extended to 5 rounds of AES, by appending one more round at the end.

[DKR97] J. Daemen, L. R. Knudsen, and V. Rijmen. "The Block Cipher Square". In: *FSE '97*. Vol. 1267. LNCS. Springer, 1997, pp. 149–165. DOI: 10.1007/BFb0052343.

1–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 truncated to 128 bits.



Target short messages (see figure); ignore the padding for simplicity, and use the following round-reduced versions of the KECCAK-f[1600] permutation:

(a) 4 Rounds (8 Points): Choose a suitable cube size, perform the precomputation to recover the superpoly coefficients, and finally collect enough linear equations to recover (most of) your secret key K.

(b) 5 Rounds (4 Points): Extend your attack to 5 rounds – either use a larger cube, or try to get the additional round "for free".

Hint: To simplify the task, you may (i) increase the tag size to a maximum of 320 bits, or (ii) omit the linear layer of the first round (steps θ, ρ, π).

[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.