# Problem Set 7
# Cryptographic Hash Functions
# (Summer Term 2017)

Bauhaus-Universität Weimar, Chair of Media Security
Prof. Dr. Stefan Lucks, Eik List
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching/`

**Due Date:** 11 July 2017, 1:30 PM, via email to `eik.list(at)uni-weimar.de`.

**Goal of this Problem Set:** Understand and analyze SHA-3 candidates

### Task 1 – CubeHash (4 Credits)

In the lecture, CubeHash was introduced as one of the SHA-3 candidates. In the following, consider two variants CubeHash′ and CubeHash″, which have a slightly different round function (see Slide 235 in Section 9.3 for the original round function).

**CubeHash′:** The rotations (Steps 2 and 7) are omitted.

**CubeHash″:** The swap operations (Steps 3, 5, 8, and 10) are omitted.

Explain how these changes influence the security of the particular round functions regarding to differential cryptanalysis and the existence of symmetric states.

### Task 2 – Skein (6 Credits)

Consider the block cipher ThreeFish′-256 which is a modified variant of the block cipher ThreeFish under the SHA-3 finalist Skein-256, where the rotation constants within ThreeFish′-256 are all set to 16. So, the function Mix : $\{0,1\}^{64} \times \{0,1\}^{64} \to \{0,1\}^{64} \times \{0,1\}^{64}$ in ThreeFish′-256 is defined as

$$\begin{aligned} \text{Mix}(L,R) &:= (X,Y), \\ X &:= (L+R) \bmod 2^{64}, \\ Y &:= X \oplus (R \lll 16). \end{aligned}$$

The values $L, R, X, Y$ are all 64-bit unsigned integers. Find a non-zero differential characteristic with probability $\gg 2^{-256}$ for ThreeFish′-256 for as many rounds as possible.

### Task 3 – Zero-Sum Distinguishers (1+1+4 Credits)

Prior to this task, read the chapter on Keccak in the lecture slides. Alice has heard that Keccak is great, and therefore has developed an idea for a lightweight AES-like permutation on 80-bit inputs. She reuses the structure of the AES with the difference that her construction works on 5-bit values instead of bytes. So, ShiftRows is exactly as in the AES, MixColumns uses the same matrix, but in $\mathbb{GF}(2^5)$ with the irreducible polynomial $x^5+x^2+1$, and SubBytes uses the S-box $S : \{0,1\}^5 \to \{0,1\}^5$ of Keccak. Since she needs only a permutation, the round-key XORs are replaced by XORs with public round constants.[1]

[1] The constants are unimportant here, so you can neglect them. They shall simply thwart iterative attacks as seen in the previous problem set.

a) Find the algebraic normal form of $S$ for bit $i$ of a five-bit input $(x_4x_3x_2x_1x_0)$ (the ANF is identical for all bits).

b) Find the algebraic normal form of $S^{-1}$ for bit $i$ of a five-bit input $(y_4y_3y_2y_1y_0)$ (again, it is identical for all bits).

c) Describe *either* a distinguisher on at least 9 rounds of Alice' permutation and describe its complexity *or* explain reasonably why such attacks cannot exist.

**Bonus (+1):** Read the paragraph "Adding a free round in the middle" from `https://eprint.iacr.org/2015/030.pdf` and describe how you can extend your distinguisher by a round. Explain the complexity of your so-modified distinguisher.

**Task 4 – Bonus: The Rebound Attack (4 Credits)**
Inform yourselves about the rebound attack, e.g., from Section 5.1 in here. Describe how to find a collision on four rounds of Alice' permutation in Task 3 when used in Matyas-Meyer-Oseas mode, and explain the complexity of your attack.