# Cryptography, winter 2014/2015

PD Dr. Adrian Spalka, Dr. Daniel Loebenberger

## 5. Exercise sheet
## Hand in solutions until
## Wednesday, 03 December 2014, 23:59:59

**Exercise 5.1** (Playing with Keccak). (14+10 points)

There are three important URLs concerning Keccak (which got later SHA-3):

- Specifications summary in Pseudo Code:

  `http://keccak.noekeon.org/specs_summary.html`.

- KeccakTools:

  `http://keccak.noekeon.org/KeccakTools-3.3.zip`

- Keccak in Python:

  `http://keccak.noekeon.org/KeccakInPython-3.0.zip`

(i) Describe the main properties of Keccak. List detailed how many operation one round of the Keccak round functions needs. What do you observe? [4]

(ii) Download an implementation of Keccak in a language you feel comfortable with. [1]

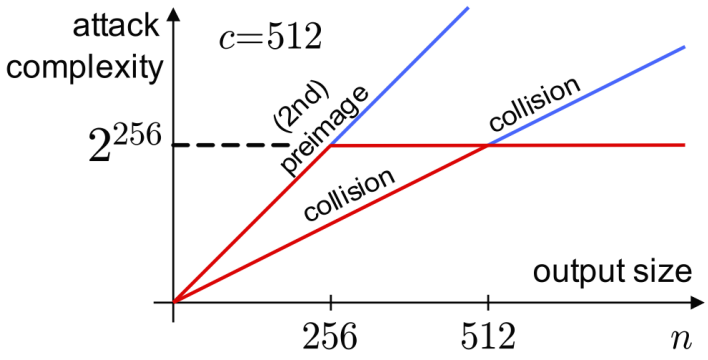
(iii) Initiate Keccak-25 with an all 0 state. How many rounds does it take until each bit has flipped at least once? [6]

(iv) Modify the round function by omitting one of the permutations and measure again the number of required rounds to have each bit flipped at least once? Make a guess before actually trying this. [3]

(v) Perform more experiments! [+10]

**Exercise 5.2** (Sponge claim). (10 points)

In the lecture we saw the following illustration of what is called the *sponge claim*:




4 (i) Explain in your own words what the illustration means.

6 (ii) Explain detailed why the claim is reasonable for the 2nd-preimage complexity if the permutation $f$ in the sponge function behaves like a random function. Hint: Argue similarly to the way we argued for generic collisions of a sponge function.