Exercise Sheet 3

Lightweight Ciphers for Hardware

Obligatory homework this week: None.
Optional homework this week: None.

Exercise 1: Hardware area consumption of the AES state
Assume that one flip-flop (bit of storage) requires 6 GE (Gate Equivalents) in hardware. How many GE does the entire AES state occupy in hardware? Remember to count the key state as well. How does this area occupation approximately translate to the physical area in mm^2 of the AES state in silicon if we assume the current 22 nm process?

Exercise 2: Hardware area consumption of cryptoraphic logic
Review the costs of some logic elements in GE from the lecture. How many GE are approximately needed to implement the following function in 4 variables:

$$f(x_1, x_2, x_3, x_4) = x_1x_2x_3 \oplus x_1x_3 \oplus x_2x_4 \oplus x_1 \oplus x_4.$$

How does this approximately translate to the physical area in mm^2 of this function f in silicon if we assume the current 22 nm process?

Exercise 3: Hardware area consumption of KATAN
The KATAN round function is identical to the KTANTAN round function, shown in the lecture. However, KATAN has a key-schedule, which consists of an 80-bit linear feedback shift register which is clocked each round. Clocking the register requires 3 XORs.
How many GE are approximately needed to implement KATAN? How does this approximately translate to the physical area in mm^2 in silicon if we assume the current 22 nm process?