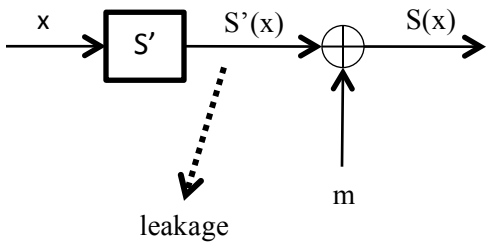
Side channel attacks: Questions

1 (Acquisition). An acquisition of power consumption for an AES encryption was performed with the sampling rate of 250 MS/s. In the power traces, we observe the correlation of power consumption with 1^{st} round intermediates around sample 84, and the correlation of power consumption with 10^{th} round intermediates around sample 154. Assuming the implementation executes one round in one clock cycle, what is the clock frequency of the device?

2 (DPA). We are recovering the full AES key with the DPA attack. After attacking the 1^{st} round, we have for each S-box a list of candidates ranked by the correlation coefficient value, with the most correlating (i.e. most probable) candidates on top. Assuming we have a standard PC at hand for the brute force attack, how many top candidates can we take from the ranked lists to find the full AES key?

3 (Countermeasures). Assume that in our device the output of a lookup table, such as an S-box, is significantly leaking through power consumption and EM radiation. We can think of the following countermeasure:



In the countermeasure, instead of the S-box S(x), we have a *masked* S-box S'(x) that returns directly the value S(x) XOR m, where m is the so-called *mask*. At some point in the implementation the value is unmasked, but the leakage of the unmasking and its results is insignificant. Assume that the mask m (and correspondingly the masked S-box S') is generated when the device is manufactured and then not changed. The attacker does not know the value of m. Is the countermeasure secure against DPA? If not, how to make it secure?

4 (Countermeasures, advanced). Assume you have timing disarrangement in the side channel traces such that the timing of the (single) leaking sample is distributed uniformly and randomly over *t* samples. How many more traces would you need to attack the device if you cannot align the traces, compared to the case with the perfect alignment?
Hint: Refer to Section 4 of the following paper: *S. Mangard. Hardware Countermeasures against DPA – A Statistical Analysis of Their Effectiveness. CT-RSA 2004*.