Memory bandwidth influence makes Cortex M4 benchmarking difficult

We might better add careful memory infrastructure characterizations to our papers or agree on one reference target for comparisons

Endress+Hauser
People for Process Automation

Diffie-Hellman Speed measurements on the M4

- FourQ, Liu et al.
  STM32F407 having 64k of tightly core-coupled memory CCM
  530k @ 168 MHz
- X25519, De Santis et al.
  STM32F411RE
  1423k, clock frequency unclear
- X25519, Fujii and Aranha
  MK20DX256VLH7 @72 MHz
  907k @ 72 MHz
- X25519, own results
  STM32L407, 611k @16 MHz, 868k@75 MHz
  Nordic nRF52832, 722k @64 MHz

How much bandwidth slowdown is present in the *other's* cycle counts?

Conclusion and suggestions

- The Cortex M4 is no longer a simple microcontroller.
- We need to consider memory bandwidth for speed benchmarking.

Suggestions:

- Maybe it's best to agree on a specific microcontroller for comparison. Let's choose a mid-size one? Suggestion: STM32F411 ?
- I also suggest to report two different cycle counts in future papers:
  1. at very low frequency (where e.g. flash memory wait states are less relevant)
  2. at maximum clock rate of the device.