Thesis/Project proposal

Name	TAKS_HLS
Contacts	Luigi Pomante <luigi.pomante@univaq.it> Walter Tiberti <walter.tiberti@graduate.univaq.it> Giacomo Valente <giacomo.valente@univaq.it>
Type	Implementation, Research
Keywords	Cryptography, HW Digital Design, C++, HLS, FPGA, Xilinx, Zynq
Description	The thesis focus on develop a HW implementation of TAKS [1] cryptographic scheme using Xilinx High-Level Syntesis [2] [3]. The finished design shall be deployed on ZYNQ boards. Performance evaluation (using also [4]), energy-consumption, side-channel resistance and comparison with the software version are requested. Details: - Study [1], [2][3] - Initial Design (C++) - Conversion to HLS - Synthesis, deployement and validation - Performance retrieval
Expected Duration	3-4 months
References (Online)	[1] https://ieeexplore.ieee.org/document/4660137 [2] https://www.xilinx.com/products/design-tools/vivado/integration/esl-design.html [3] https://www.xilinx.com/support/documentation/sw_manuals/xilinx2017_1/ug871-vivado-high-level-synthesis-tutorial.pdf [4] https://ieeexplore.ieee.org/document/7445360
References (Attached)	