Cybersecurity Institute
Univ. Grenoble Alpes

Internship: Design and Study of Fast AES-256 and SHA-3 Implementations Resistant against Side Channel and Fault Attacks

Reference	CYBERINSTITUTE-INT-20001
Description	Data protection, in terms of confidentiality and/or integrity, is becoming fundamentally important in an increasing number of domains. These properties are usually guaranteed through cryptographic primitives such as symmetric ciphers and hashing algorithms. The evolution of society pushes for strong, fast, and robust implementations of these functions, which may be implemented in hardware to optimize overall performance. On the other hand, designers must take care that the implementations are not vulnerable to the so-called implementation attacks, based for example on the analysis of power consumption, or of faulty results. During this internship, the candidate will need to design a hardware accelerator for AES-256 and SHA-3, the current state-of-the-art algorithms for symmetric encryption and hashing. The traditional performance figures for hardware implementations will be taken into consideration (resources, latency, throughput, power consumption), as well as the robustness against implementation attacks, both passive (side channels) and active (fault injections). Suitable countermeasures against these attacks will be proposed, such as masking or redundancy schemes in order to thwart the attacks. Then, these countermeasures will be implemented and their impact on performance evaluated. An implementation flow targeting both ASIC and FPGA designs may be taken into consideration. Context: The Grenoble Alpes Cybersecurity Institute – in short, Cyber@Alps – is a project selected in 2017 by the Cross-Disciplinary Program (CDP) of the IDEX Univ. Grenoble Alpes and aims at undertaking ground-breaking interdisciplinary research in order to address cybersecurity and privacy protection challenges. Our main technical focus are on cost effective secure elements, security of critical infrastructures all along their life cycle, vulnerability analysis and global challenges in terms of risk analysis and validation of large systems, including practical resilience across the industry and the society. Our approach to cybersecurity is holistic, encompassing technical, legal, law-enforcement, economic, social, diplomatic, military and intelligence-related aspects with strong partnerships with the private sector and robust national and international cooperation with leading institutions in France and abroad (https://cybersecurity.univ-grenoble-alpes.fr)
Prerequisites	Digital design, VHDL/Verilog strongly encouraged; knowledge of hardware security is a plus

Tutors	Paolo MAISTRI, CR, CNRS/TIMA ; paolo.maistri@univ-grenoble-alpes.fr
Applications	Please send your resume, application letter with two recommendations (including education director), first year master's degree grades (mandatory) and second year grades (if possible) to cyberalps-contact@univ-grenoble-alpes.fr For more information on the internship, please contact [paolo.maistri@univ-grenoble-alpes.fr]
Location	TIMA Laboratory, 46 avenue Félix Viallet, 38000 Grenoble
Starting date	Feb-2020
Duration	5 to 6 months
Allowance	In accordance with existing regulations (approx. 560€/month). Part of travel expenses can be covered.

financed by
IDEX Université Grenoble Alpes