Design Automation for Security: History and Perspectives

Prof. Francesco Regazzoni

University of Amsterdam

Venerdì 9 febbraio 2024 - ore 12:00

Dipartimento di Scienze Umanistiche e Sociali

Aula Pissarello B

ABSTRACT

Physical attacks exploit the physical weaknesses of cryptographic devices to reveal the secret information stored on them. Countermeasures against these attacks are often considered only in the later stages of the full design flow, and applied manually by designers with strong security expertise. This approach, however, negatively affects the robustness, the cost, and the production time of secure devices. A more effective way to implement secure cryptographic algorithms would enable the automatic application of side channel countermeasures and would support the verification of their correct application. This talk will revise and summarize the research efforts in this important research direction, from the first works implementing hardware design flow for security to the initial steps of automatically driving design tools using security variables, and it will highlight future research direction in design automation for security.

UNISS Università degli Studi di Sassari — Dipartimento di Scienze Umanistiche e Sociali

AIMet Lab — Artificial Intelligence and Formal Methods Lab

SECURED EU Project