Jaouhar Fattahi, Ph.D

About the speaker and short CV:

Jaouhar Fattahi is currently with Laval University in Quebec City, Canada, as an associate professor. He received his Ph.D. on cryptographic protocol security from Laval University in October 2015. He completed his postdoctoral training at the Valcartier Research Center for the Canadian Armed Forces in the field of cybersecurity. He is also a computer engineer since 1995. Jaouhar Fattahi is the author of the theory of witness functions for security verification of cryptographic protocols. He now specializes in reverse engineering and machine and deep learning applied to security and cybersecurity. He is also a member of the IEEE.

Analysis of cryptographic protocols in theory of witness functions

Presentation abstract:

Encrypting the messages exchanged in a protocol is not enough to guarantee the confidentiality of the data exchanged. Indeed, a man in the middle can fool the rules of the protocol to know what they are not entitled to. An appropriate method of analyzing protocols must be used. There are several effective methods such as the witness functions method developed at LSI of Laval University. We will talk about the theory of witness functions in the analysis of cryptographic protocols and the excellent results that have been achieved with these functions regarding their security.

Links:

- https://dblp.uni-trier.de/pid/97/11071.html
- https://www.ift.ulaval.ca/departement-et-professeurs/professeurs-et-personnel/professeurs-associes/