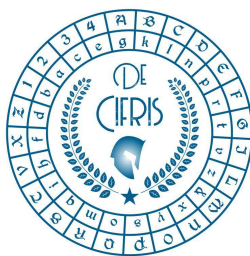


# De Cifris Athesis



UNIVERSITÀ DEGLI STUDI  
DI TRENTO

Dipartimento di Matematica



ICT  
CENTER FOR INFORMATION AND  
COMMUNICATION TECHNOLOGY

**Thursday 25<sup>th</sup> March 2021 – at 10:00 a.m.**  
**Online Seminar via Zoom**

**Irene Villa**

**Università degli Studi di Trento**

## **Analysis, classification and construction of APN Boolean functions**

**Abstract:** This talk will be focused on APN Boolean functions, which are optimal cryptographic functions. I will give an overview of this class of functions and then present some recent results. In particular, I will present results on new construction methods for APN functions and on equivalence among known APN families.

**Iscrizione all'evento online da effettuare entro il 24 marzo tramite il seguente link:**

**[click here](#)**

Gli iscritti riceveranno l'ID Zoom un'ora prima dell'inizio dell'evento.

**Contact person:** Massimiliano Sala

**CONTATTI**

Associazione De Componendis Cifris

[segreteria@decifris.it](mailto:segreteria@decifris.it)