DIPARTIMENTO MATEMATICA
Dipartimento di Matematica "Tullio Levi-Civita"

Associazione
«Patavina Mathesis»

Mathesis Venezia

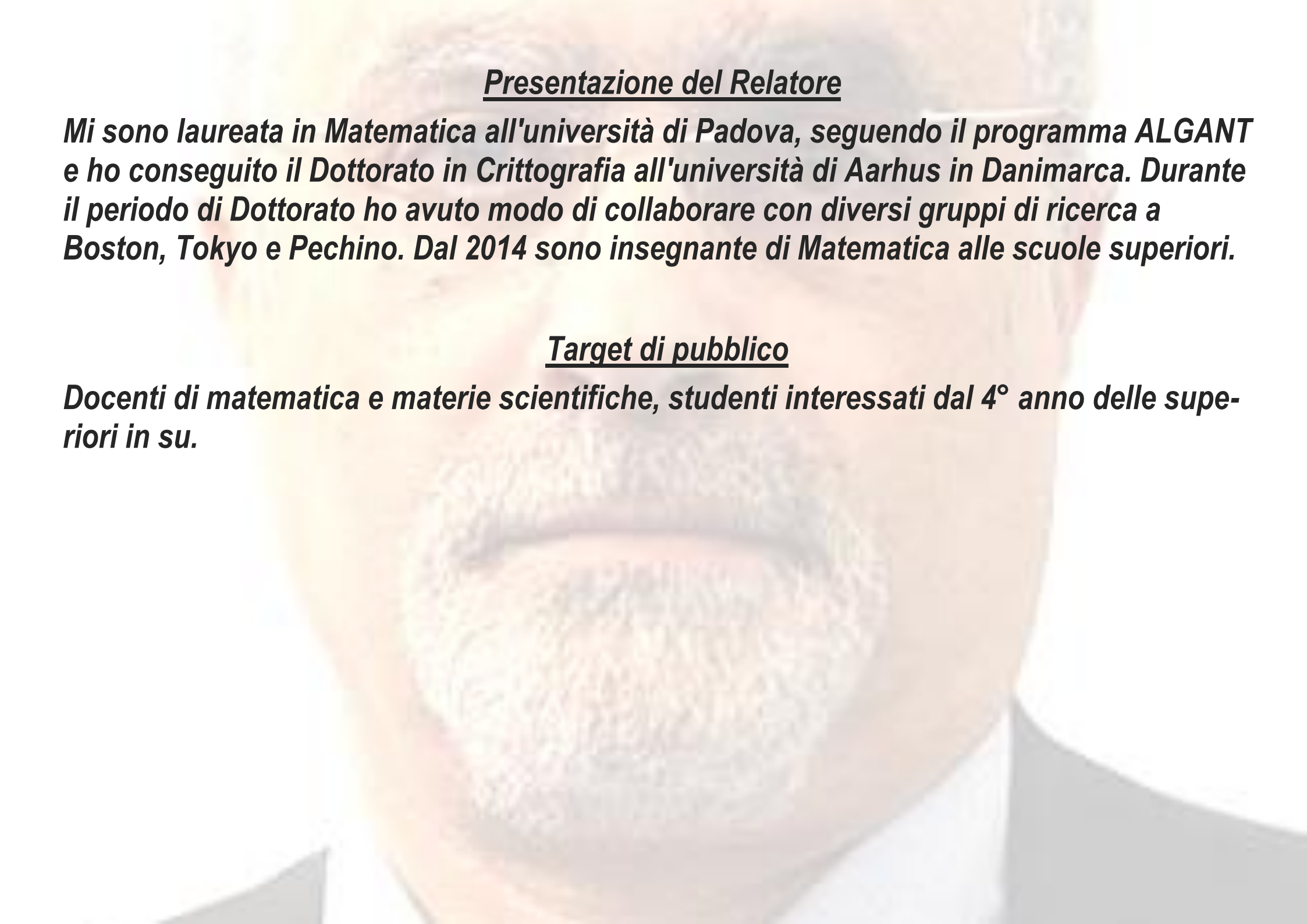
Venerdì 9 aprile 2021 17.30 - 19.00

Conferenza online di *Angela Zottarel*

UN ESEMPIO DI CRITTOGRAFIA MODERNA : EL GAMAL

Abstract

Con l'avvento del computer, la crittografia ha avuto accesso ad un nuovo potente strumento che, da un lato, offriva la possibilità di codificare molto più velocemente, ma dall'altro permetteva anche lo sviluppo di programmi che potessero rompere quasi ogni tipo di sistema noto. Ci si è trovati, quindi, nella necessità di inventare nuovi sistemi che offrissero sicurezza (dimostrabile) anche alla luce delle nuove tecnologie. Questo è stato fatto attraverso un'impostazione più matematica della crittografia e attingendo a strumenti matematici come la teoria dei numeri e la teoria dei gruppi. In questa conferenza presentiamo la definizione moderna di crittosistema e spieghiamo in che modo se ne può dimostrare la sicurezza. Faremo anche un esempio di crittosistema moderno, il sistema El Gamal, introducendo le nozioni di base di teoria dei gruppi e aritmetica modulare su cui si basa.



Presentazione del Relatore

Mi sono laureata in Matematica all'università di Padova, seguendo il programma ALGANT e ho conseguito il Dottorato in Crittografia all'università di Aarhus in Danimarca. Durante il periodo di Dottorato ho avuto modo di collaborare con diversi gruppi di ricerca a Boston, Tokyo e Pechino. Dal 2014 sono insegnante di Matematica alle scuole superiori.

Target di pubblico

Docenti di matematica e materie scientifiche, studenti interessati dal 4° anno delle superiori in su.