ALPEN-ADRIA UNIVERSITÄT KLAGENFURT

INVITATION TO THE PRESENTATION ABOUT THE WORK-PLACEMENT

Low-weight digit expansions with odd digits

Dunja Pucher | Universität Klagenfurt

Chaired by Clemens Heuberger | Department of Mathematics

Wednesday, 2 December 2020 | 16:15–17:00

https://classroom.aau.at/b/heu-x6a-ree-2xg

ABSTRACT

In my research I deal with radix-2 joint expansions for pairs of integers and for the digit sets containing consecutive odd digits as well as the digit zero. More specifically, I gave a right-to-left algorithm which builds minimal weight representations for the digit set $D = \{0, \pm 1, \pm 3\}$ and proved its optimality.

In my work placement I had two tasks:

The first task was to prepare and give a talk about the given algorithm on the 20th Central European Conference on Cryptology, which was held in Zagreb in June 2020.

The second task was to test the algorithm with some other digit sets which contain consecutive odd digits as well as the digit zero. Among others, I gave a generalized version of the Joint Sparse Form for the digit set $D = \{0, \pm 1\}$ and arbitrary dimensions. Furthermore, I gave an approximation algorithm for the digit set $D = \{0, \pm 1, \pm 3, \pm 5\}$ which has an offset to the minimal weight of 0.06%.

We hope to see you there!