## Chair of "Secure Digital Circuits"



# Use of Non-Binary LDPC Codes over Division Near Rings for Physical Layer Security

## Introduction

While most security mechanisms operate on higher communication layers, physical-layer security is a promising candidate to raise the overall security of communication channels. Recently, promising physical-layer approaches in which channel codes including binary Low-Density Parity-Check (LDPC) and Polar codes have been proposed for a secure data communication.

#### Closed, Non-Abelian inverse Commu-Group tative element Closed. DNR Division inverse over Near **Multiplicative Group** Soint Pelayati Ring element SNG Non-0 Commu 5 tative dВ ubtractiv Abelian Finite Near 0.05 dB Group Fields Group

Algebraic field options for physical layer

security mechanisms

Addditive Group

# Short Project Description

The goal of this project is to analyze non-binary LDPC codes over division near rings with respect to security. Therefore, an existing C model of an unsecure communication channel, in which error correction is done using a non-binary LDPC code over division near rings, shall be extended towards a secure communication channel featuring physical-layer security.

## Prerequisites

- Interest in signal processing and digital baseband algorithms
- Basic knowledge in C is helpful

## What you will learn

After the project you will be familiar with the non-binary LDPC decoding algorithm as well as the basic concepts of physical layer security.

## Contact

matthias.korb@unibw.de