

Polar Coding and Secrecy Performance Analysis at Finite Blocklengths

Hsuan-Yin Lin

November 29, 2024

Polar codes, introduced by Arikan, are the first class of linear block codes proven to achieve channel capacity for binary-input memoryless channels (BI-MCs) while offering low-complexity encoding, decoding, and practical constructions. In this talk, we will provide a brief introduction to polar codes and their extensions, including pre-transformation techniques such as polarization-adjusted convolutional (PAC) codes. Recently, PAC codes have been proposed and shown significant advantages for one-to-one noisy BI-MCs, achieving performance close to the finite-blocklength normal approximation bound. In this work, we explore non-asymptotic theoretical results on the secrecy rate and design secrecy codes using PAC codes at short blocklengths in the presence of eavesdroppers, employing binary polarization kernels different from Arikan's original kernels.