Linear Complementary Dual Codes and Linear Complementary Pair of Codes

Cem Güneri

Sabancı University

Linear complementary dual (LCD) codes and linear complementary pair (LCP) of codes have drawn attention in recent years due to their cryptographic applications. We will talk about one such motivation from cryptography, namely the fault injection attack. Then, we will survey important results on such codes and present some of our recent findings on the topic.