SEMINARIO

Selcen Sayici

Sabancı University, Turquía

On Abelian Linear Complementary Pair Of Codes

Abstract: Linear Complementary Dual(LCD) and Linear Complementary Pair(LCP) of codes have been intensively studied recently due to their applications in many areas such as cryptography. It has been shown that they can help to improve the security of the information in order to be protected against some attacks.

The security parameter for a linear complementary pair (C, D) of codes is defined to be the minimum of the minimum distances $d(C)$ and $d(D^{\perp})$. For the LCD case, this parameter is simply d(C), since $D^{\perp} = C$. Recently, Carlet et al. showed that if C and D are both cyclic or both 2D cyclic LCP of codes, then C and $D^{\perp}$ are equivalent codes. Hence the security parameter for cyclic and 2D cyclic LCP of codes is simply $d(C)$. We generalize this result to nD cyclic (abelian) LCP of codes. The proof of Carlet et al. for the 2D cyclic case uses the trace representation of the codes. Our proof for the generalization is based on the zero sets of the ideals corresponding to nD cyclic codes.

Seminario IMUVA. Edificio LUCIA
Jueves 14 de Marzo de 2019 (13:00)
Organiza: GIR SINGACOM