Reading list for INF347

Selected topics in cryptology

(all literature is available online)

L. Budaghyan. Construction and Analysis of Cryptographic Functions. Springer Verlag, 2015.

L. Budaghyan. The Equivalence of AB and APN Functions and Their Generalizations. VDM verlag, 2008.

C. Carlet. Vectorial Boolean Functions for Cryptography. Chapter of the monography Boolean Methods and Models, Cambridge University Press, pp. 398-472, 2010.

C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes. Chapter of the monography Boolean Methods and Models, Cambridge University Press, 2010.

T. Cusick, P. Stanica. Cryptographic Boolean Functions and Applications. Elsevier, 2017.

R. Lidl, H. Niederreiter. Introduction to finiete fields and their applications. Cambride University Press, 1997.