Boolean Functions For Cryptography And Error Correcting Codes

Read/Download
The study of monotonicity and negation complexity for Boolean functions has been prevalent in iii) Error-correcting codes with optimal distance parameters require log n−O(1) negations (again. Thus the S-boxes used in lightweight cryptography should (4) Carlet, C., Boolean functions for cryptography and error correcting codes, In: Boolean Models. 1 Examples, 2 Properties, 3 Error detection and error correction, 4 History and Thus a code with minimum Hamming distance d between its codewords can detect at least d − 1 errors. Boolean functions play a critical role in cryptography as well as in the design of error-correcting codes.