Normal bases over finite fields have been widely used in many applications of cryptography and coding theory. They are also important for Frobenius mapping and efficient for the implementation of the arithmetic of finite fields. Let

Abstract

References

Normal Elements using Trace Mapping over Finite Fields

170-183.

Index Terms

Computer Science Information Systems

Keywords

Normal basis, Trace function, Hamming weight, Symmetric vector.