

Year: 2012

Vol.: 80

Fasc.: 3-4

Title: Measures of pseudorandomness of families of binary lattices, II (A further construction)

Author(s): Katalin Gyarmati, Christian Mauduit and András Sárközy

In Part I of this paper we extended the notions of family complexity, collision and avalanche effect from one dimension to n dimensions, i.e., from binary sequences to binary lattices. Then we considered a large family of binary lattices with strong pseudorandom properties which had been constructed by using quadratic characters of finite fields, and we showed that this family also possesses a nice structure in terms of these notions. In Part I we considered a large family of binary sequences with strong pseudorandom properties constructed by using additive characters and we extended it to n dimensions, i.e., to binary lattices. In this paper we will show that these binary lattices possess strong pseudorandom properties, and their family also possesses a nice structure in terms of family complexity, collision and avalanche effect.

Address:

Katalin Gyarmati
Eötvös Loránd University
Department of Algebra
and Number Theory
Pázmány Péter sétány 1/C
H-1117 Budapest
Hungary

Address:

Christian Mauduit
Institut de Mathématiques de Luminy
CNRS, UMR 6206
163 avenue de Luminy, Case 907
F-13288 Marseille Cedex 9
France

Address:

András Sárközy
Eötvös Loránd University
Department of Algebra
and Number Theory
Pázmány Péter sétány 1/C
H-1117 Budapest
Hungary