Generalised Rijndael

Sergi Blanch-Torné[1], Ramiro Moreno Chiral[2], Francesc Sebé Feixa[2]

[1] Escola Politècnica Superior, Universitat de Lleida. Spain.
sblanch@alumnes.udl.es
[2] Departament de Matemàtica. Universitat de Lleida. Spain.
{ramiro,fsebe}@matematica.udl.es

August 21, 2012

Abstract. [3] This is the abstract

Keywords: Cryptography, Symmetrics, Rijndael

1 Introduction

2 Approach to the Rijndael Schema

2.1 Mathematical preliminaries

2.2 Design

3 Generalising the schema

3.1 key expansion

3.2 Rounds

3.3 subBytes

sboxes

3.4 shiftColumns

3.5 mixColumns

3.6 addRoundKey

4 Paramenter convinations

5 New useful sizes for rijndael

[3] Partially founded by the Spanish project MTM20__-_____-___-__