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 22, 2012

Abstract. [3] This is the abstract

Keywords: Cryptography, Symmetrics, Rijndael

1 Introduction

[1] [2] [3] [4]

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

[5]

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

References

1. J. Daemen and V. Rijmen, "The block cipher rijndael," in *Proceedings of the The International Conference on Smart Card Research and Applications*, CARDIS '98, (London, UK, UK), pp. 277–284, Springer-Verlag, 2000.
2. J. Daemen, J. Daemen, J. Daemen, V. Rijmen, and V. Rijmen, "Aes proposal: Rijndael," 1998.
3. J. Schaad and R. Housley, "Advanced Encryption Standard (AES) Key Wrap Algorithm." RFC 3394 (Informational), Sept. 2002.
4. A. T. Federal, "Processing standards publication 197."
5. J. Daemen and V. Rijmen, "Efficient block ciphers for smartcards," in *Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology*, WOST'99, (Berkeley, CA, USA), pp. 4–4, USENIX Association, 1999.