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 Design

3 Generalising the schema

3.1 key expansion

3.2 Rounds

3.3 subBytes

How to build different SBoxes

3.4 shiftColumns

3.5 mixColumns

3.6 Operate in a polinomial ring, with coeficients in a polinomial field

$$\frac{\mathbb{F}_{2^n}[y]}{m(y)}$$

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

Algorithm 1 KeyExpansion

```
INPUT: byte k[nRows*nColumns], nRounds, nRowns, nColumns, wSize
OUTPUT: word w[nRouns*(nRows+1)]
i := 0
while i¡nColumns do
    w[i] := word(k[nRows*(i+c) for c in range(nColumns)])
end while
i := nColumns
while i¡nRouns*(nRows+1) do
    temp := w[i-1]
    if i mod nColumns == 0 then
        temp := SubWord(RotWord(temp)) $\oplus$ Rcon[i/nColumns]
    else
        temp := SubWord(temp)
    end if
    w[i] := w[i-nColumns] $\oplus$ temp
    i++
end while
```

where $m(y)$ is a composed polinomial of degree r columns. This gives a polinomial ring. The coeficients of this polinomial ring are elements of a polinomial field

$$\mathbb{F}_{2^n} = \frac{\mathbb{F}_{2^2}[x]}{m(x)}$$

where $m(x)$ is irreductible and gives a polinomial field. Standard rijndael (AES) uses a circulan invertible matrix for this to simplify and speed up the operations in the ring.

3.7 addRoundKey

4 Parameter combinations

5 New useful sizes for Rijndael

[5]

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. "Specification for the advanced encryption standard (aes)." Federal Information Processin Standards Publication 197, 2001.
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.

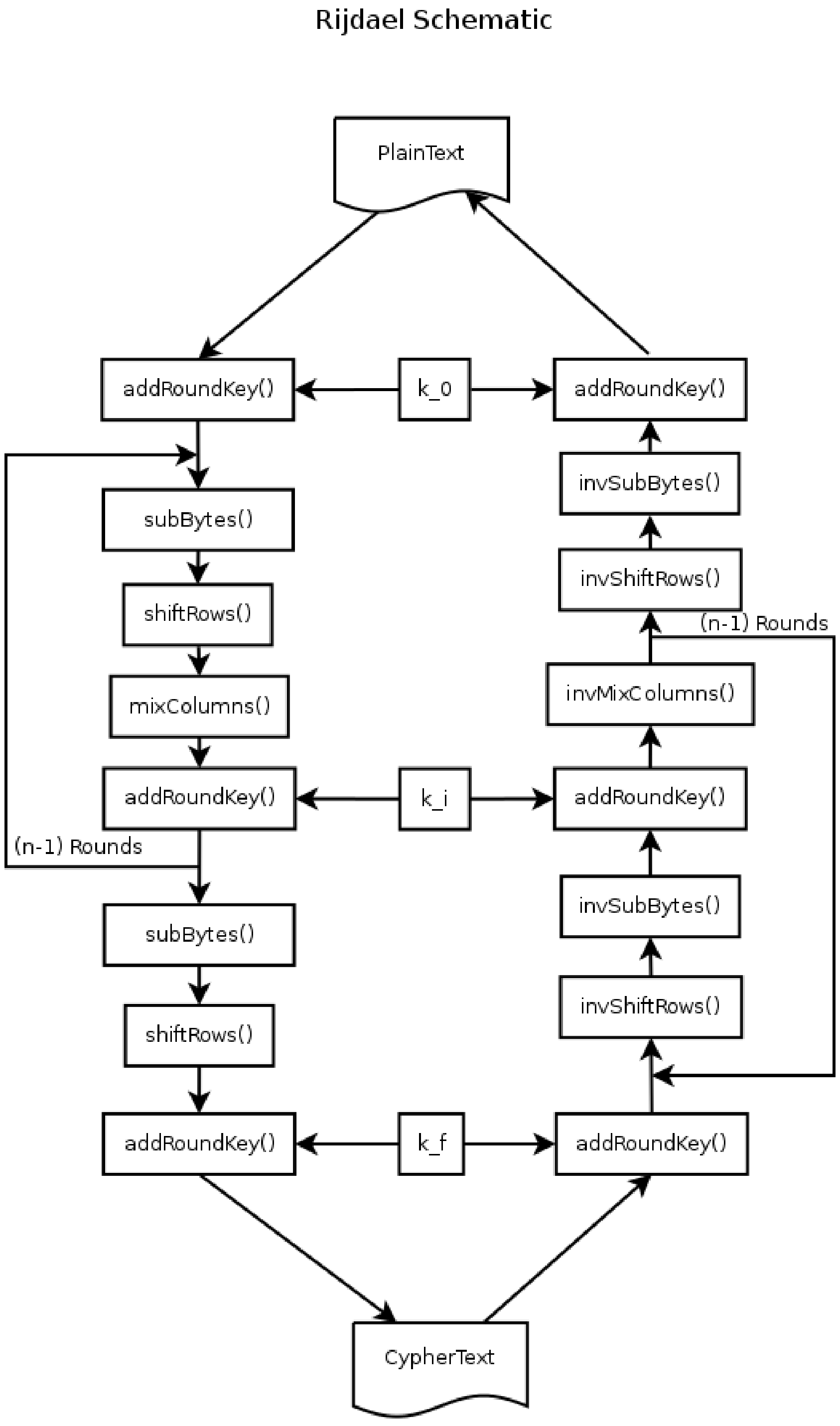

Fig. 1. rijndael diagram

$$k = k_0, k_1, \cdots, k_n = \begin{bmatrix} k_{0_{0,0}} & k_{0_{0,1}} & k_{0_{0,2}} & k_{0_{0,3}} \\ k_{0_{1,0}} & k_{0_{1,1}} & k_{0_{1,2}} & k_{0_{1,3}} \\ k_{0_{2,0}} & k_{0_{2,1}} & k_{0_{2,2}} & k_{0_{2,3}} \\ k_{0_{3,0}} & k_{0_{3,1}} & k_{0_{3,2}} & k_{0_{3,3}} \end{bmatrix} \begin{bmatrix} k_{1_{0,0}} & k_{1_{0,1}} & k_{1_{0,2}} & k_{1_{0,3}} \\ k_{1_{1,0}} & k_{1_{1,1}} & k_{1_{1,2}} & k_{1_{1,3}} \\ k_{1_{2,0}} & k_{1_{2,1}} & k_{1_{2,2}} & k_{1_{2,3}} \\ k_{1_{3,0}} & k_{1_{3,1}} & k_{1_{3,2}} & k_{1_{3,3}} \end{bmatrix} \cdots \begin{bmatrix} k_{n_{0,0}} & k_{n_{0,1}} & k_{n_{0,2}} & k_{n_{0,3}} \\ k_{n_{1,0}} & k_{n_{1,1}} & k_{n_{1,2}} & k_{n_{1,3}} \\ k_{n_{2,0}} & k_{n_{2,1}} & k_{n_{2,2}} & k_{n_{2,3}} \\ k_{n_{3,0}} & k_{n_{3,1}} & k_{n_{3,2}} & k_{n_{3,3}} \end{bmatrix}$$

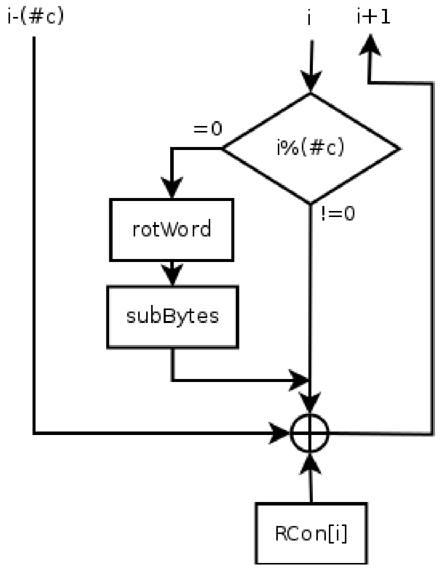

Fig. 2. Block diagram of the construction of the rijndael key expansion