More Dual Rijndaels

Håvard Raddum

Dep. of Informatics, The University of Bergen, P.O.box 7800, 5020 Bergen, Norway

Abstract. It is well known that replacing the irreducible polynomial used in the AES one can produce 240 dual ciphers. In this paper we present 9120 other representations of $GF(2^8)$, producing more ciphers dual to the AES. We also show that if the matrix used in the S-box of Rijndael is linear over a larger field than $GF(2)$, this would have implications for the XSL attack.

1 Introduction

The cipher Rijndael [1] has been selected by NIST as the AES. Most of the operations in Rijndael are based on the field $GF(2^8)$, and several researchers have made comments on the algebraic structures found in the cipher [3, 4, 5]. At ASIACRYPT 2002 Barkan and Biham [5] showed that the ciphers produced when changing the polynomial used in AES are duals of Rijndael. In this paper we construct many more duals of the AES.

Also at ASIACRYPT 2002 Courtois and Pieprzyk [6] described a possible attack on the AES, using a large system of equations. We will show that one of the dual ciphers could produce a much smaller system, that should be easier to solve. However, we have checked that the matrix used in the affine transformation in the S-box is not among those which would simplify the system of equations.

At EUROCRYPT 2003 Biryukov *et al.* [7] presented a tool for finding affine equivalent S-boxes. This can be used to find 2040 pairs of affine mappings that can be inserted in the AES, without changing the permutation induced by the cipher. By replacing the field polynomial in the AES with one of the 30 other irreducible polynomials, one is likely to be able to produce as many as 61,200 different versions of the duals of the AES found in [5]. This class can probably be extended using the duals presented here.

In Section 2 we give a brief description of Rijndael, and the definition of a dual cipher. In Section 3 we show how to construct 1170 different representations of $GF(2^8)$, each one resulting in 8 ciphers dual to the AES. In Section 4 we check whether the system of equations in the XSL-attack can be simplified. Conclusions are made in Section 5.

2 Description of Rijndael

We here give a brief description of Rijndael, omitting the key schedule. A more detailed description can be found in [1].

H. Dobbertin, V. Rijmen, A. Sowa (Eds.): AES 2004, LNCS 3373, pp. 142–147, 2005.

Rijndael is a 128-bit block cipher with key sizes of 128, 192 or 256 bits. The cipher consists of a round function that is repeated 10, 12 or 14 times according to the length of the key. The cipher block and the round keys are viewed as 4×4-matrices of bytes. In some operations these bytes are viewed as elements of $GF(2^8)$, as well as 8-bit strings. The irreducible polynomial over $GF(2)$ used to represent $GF(2^8)$ is $x^8 + x^4 + x^3 + x + 1$.

There are four operations in the round function of Rijndael. These are used in the following order:

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey

SubBytes replaces each byte of the cipher block. Each byte is first replaced by its inverse, when viewed as an element of $GF(2^8)$ ($0^{-1} = 0$), and then passed through an affine transformation $Ax + b$ as an 8-bit vector. The constants A and b are

$$A = \begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix}, \qquad b = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

ShiftRows takes row i of the cipher block, containing four bytes, and shifts it i positions to the left. The top row is row 0 and the bottom is row 3.

MixColumns views the cipher state as a 4×4-matrix over $GF(2^8)$, and pre-multiplies it with a constant 4×4-matrix with elements from $GF(2^8)$.

AddRoundKey simply xors the cipher block with the key for the current round.

An AddRoundKey is applied to the plaintext before the first round, and in the last round MixColumns is removed.

2.1 Dual Ciphers

We give here the definition of a dual cipher from [5].

Definition 2.1. *Two ciphers E and E' are called dual ciphers if there exists invertible transformations f, g and h such that*

$$\forall P, K \qquad f(E_K(P)) = E'_{g(K)}(h(P)).$$

In the case for Rijndael in this paper we will have $f = g = h$. The transformation f will be an isomorphism of $GF(2^8)$ applied on all 16 bytes in the cipher block in parallel.

3 Different Representations of $GF(2^8)$

The designers of Rijndael chose the irreducible polynomial $r(x) = x^8 + x^4 + x^3 + x + 1$ to construct $GF(2^8)$. In the following let α be a root of $r(x)$. Elements of $GF(2)[\alpha]$ (all sums and products of elements from $GF(2) \cup \{\alpha\}$) may be written as polynomials in α over $GF(2)$, with degree at most 7. The elements of $GF(2^8)$ are sometimes regarded as 8-bit vectors, with the natural mapping

$$c_7\alpha^7 + \ldots + c_1\alpha + c_0 \longleftrightarrow (c_7, \ldots, c_1, c_0).$$

When an element of $GF(2^8)$ is written as a column vector c_0 is at the top and c_7 is at the bottom.

3.1 Dual Ciphers by Replacing $r(x)$

There are 30 irreducible polynomials of degree 8 over $GF(2)$. As pointed out in [5], we may define β to be a root of any one of these polynomials, and construct $GF(2^8) = GF(2)[\beta]$. The isomorphism ϕ between $GF(2)[\alpha]$ and $GF(2)[\beta]$ is established when we find a root of $r(x)$ in $GF(2)[\beta]$, and let this root be the image of α.

This isomorphism is a linear mapping. Let M_ϕ be the 8×8-matrix over $GF(2)$ whose column i is $\phi(\alpha^i)$, where column 0 is the leftmost column and column 7 is the rightmost column. Then $\phi(a)$ can be computed as $\phi(a) = M_\phi \cdot a$, where $a \in GF(2)[\alpha]$ is written as a column vector.

Denote encryption of plaintext P under key K using Rijndael by $E_K(P)$. Let the cipher we get by replacing all constants in $GF(2^8)$ in Rijndael by their image under ϕ, and replacing A with $M_\phi A M_\phi^{-1}$ be called E'. Then we have the duality [5]:

$$\phi(E_K(P)) = E'_{\phi(K)}(\phi(P)),$$

where we understand ϕ to be applied to each of the $GF(2^8)$-elements in the blocks P, K and $E_K(P)$.

Since there are 8 different roots of $r(x)$ in $GF(2^8)$, we get 8 different isomorphisms between $GF(2)[\alpha]$ and each representation of $GF(2^8)$. With 30 irreducible polynomials of degree 8 over $GF(2)$ we therefore get a total of 240 different matrices M_ϕ.

3.2 Other Representations of $GF(2^8)$

There are other ways of constructing $GF(2^8)$ than by using an irreducible polynomial of degree 8 over $GF(2)$. This is shown by the following example.

First we create $GF(2^2) = GF(2)[\beta]$ with $\beta^2 + \beta + 1 = 0$. Then we can make $GF(2^8)$ with $t(x) = x^4 + \beta x^3 + x + (\beta + 1)$, an irreducible polynomial of degree 4 over $GF(2)[\beta]$. Defining γ to be a root of $t(x)$, the elements of $GF(2^8)$ can be written as polynomials in γ of degree at most 3 with coefficients from $GF(2)[\beta]$. Writing elements of $GF(2^2)$ as polynomials in β of degree at most 1 over $GF(2)$, we get a natural mapping between 8-bit strings and elements of $GF(2)[\beta, \gamma]$:

$$(c_7\beta + c_6)\gamma^3 + (c_5\beta + c_4)\gamma^2 + \ldots + (c_1\beta + c_0) \longleftrightarrow (c_7, \ldots, c_0). \qquad (1)$$

With this mapping the isomorphism $\phi : GF(2)[\alpha] \longrightarrow GF(2)[\beta, \gamma]$ can now be realized as a matrix-multiplication in the same way as in the single extension case. We find a root of $r(x)$ in $GF(2)[\beta, \gamma]$ and let this element be $\phi(\alpha)$. Then $M_\phi = [1, \phi(\alpha), \phi(\alpha^2), \ldots, \phi(\alpha^7)]$.

3.3 All Possible Representations of $GF(2^8)$ Using Irreducible Polynomials

Here we will show that there are 1170 different representations of $GF(2^8)$ using roots from irreducible polynomials. We have the following inclusions of subfields of $GF(2^8)$:

$$GF(2) \subset GF(2^2) \subset GF(2^4) \subset GF(2^8).$$

This induces four different chains of fields starting with $GF(2)$ and ending in $GF(2^8)$, these chains are listed below. The number above an arrow in $GF(2^i) \xrightarrow{n} GF(2^{di})$ means there are n irreducible polynomials of degree d over $GF(2^i)$.

- $GF(2) \xrightarrow{30} GF(2^8)$: 30 representations.
- $GF(2) \xrightarrow{1} GF(2^2) \xrightarrow{60} GF(2^8)$: 60 representations.
- $GF(2) \xrightarrow{3} GF(2^4) \xrightarrow{120} GF(2^8)$: 360 representations.
- $GF(2) \xrightarrow{1} GF(2^2) \xrightarrow{6} GF(2^4) \xrightarrow{120} GF(2^8)$: 720 representations.

Adding the numbers together we get 1170 representations of $GF(2^8)$.

The mapping between 8-bit strings and field elements for the last two chains can be done as follows.

$GF(2) \longrightarrow GF(2^4) \longrightarrow GF(2^8)$: Let β be a root of an irreducible polynomial of degree 4 over $GF(2)$, and let γ be a root of an irreducible polynomial of degree 2 over $GF(2)[\beta]$. The conversion is then

$$(c_7\beta^3 + \ldots + c_4)\gamma + (c_3\beta^3 + \ldots + c_0) \longleftrightarrow (c_7, \ldots, c_0).$$

$GF(2) \longrightarrow GF(2^2) \longrightarrow GF(2^4) \longrightarrow GF(2^8)$: Let β be a root of $x^2 + x + 1$, γ a root of an irreducible polynomial of degree 2 over $GF(2)[\beta]$, and δ a root of an irreducible polynomial of degree 2 over $GF(2)[\beta, \gamma]$. The mapping becomes

$$((c_7\beta + c_6)\gamma + (c_5\beta + c_4))\delta + ((c_3\beta + c_2)\gamma + (c_1\beta + c_0)) \longleftrightarrow (c_7, \ldots, c_0).$$

For each representation there are 8 choices for the element $\phi(\alpha)$. In total we then get $8 \cdot 1170 = 9360$ matrices M_ϕ yielding isomorphisms, and so 9360 duals of the AES. We have generated all these matrices, and checked that they are all different (However, it can be shown that there are 60 pairs of matrices $\{M, M'\}$ such that the first 4 columns of M and M' are equal).

It should be noted that the idea of constructing $GF(2^8)$ using two field extensions and applying it to Rijndael is not new. It has been done in [8], for the purpose of making an efficient hardware implementation of inversion in $GF(2^8)$.

4 Implications for the XSL-Attack

The XSL attack is described in [6]. The basis of the attack is the fact that the non-linear part of the S-box in Rijndael is inversion in the field $GF(2^8)$. If X is the input to the inversion and Y is the output, we have the relation $XY = 1$ (except for $X = 0$). By writing X as $x_7\alpha^7 + \ldots + x_0$ and Y as $y_7\alpha^7 + \ldots + y_0$, the expression

$$(x_7\alpha^7 + \ldots + x_0)(y_7\alpha^7 + \ldots + y_0) = 0 \cdot \alpha^7 + \ldots + 0 \cdot \alpha + 1$$

will give us 8 quadratic equations in the variables $x_0, \ldots, x_7, y_0, \ldots, y_7$.

4.1 Brief Summary of the XSL Attack

At some point in each round, we give variable names to the bits of the cipher block. Since all the operations in Rijndael except the field inversion are linear over $GF(2)$, the input and output of the inversion are linear expressions in these variables. By using the relation of the field inversion described above, we can create an equation system in the key bits and the intermediate ciphertext bits using one known plaintext/ciphertext pair. All of these equations will be quadratic, and for the 128-bit key case the system should define the key uniquely.

The rest of the attack is to try to solve this equation system by creating new equations using multiplication with monomials, and in the end using re-linearization. If the XSL attack works, it is important that it is faster than exhaustive search. One crucial point for the complexity of solving the system is the number of variables it contains, and for the re-linearization, the number of monomials.

4.2 Matrix in S-Box $GF(2^2)$-Linear?

Let us assume for a little while that the matrix used in the S-box of Rijndael is linear over $GF(2^2)$. The other linear operations are linear over $GF(2^8)$, and in particular over $GF(2^2)$. This means that Rijndael can be described completely in terms of $GF(2^2)$, it will never be necessary to go down to bit level in any of the operations. Since all the linear operations of Rijndael are $GF(2^2)$-linear, we can make an equation system like the one used in the XSL-attack, but now with variables and coefficients from $GF(2^2)$. Since two and two bits are melted together to form one variable, we will only get half as many variables as in the original system, and only about one fourth of the number of quadratic monomials. Since the number of monomials is significantly smaller in the system over $GF(2^2)$, and since we only have half as many variables, it should be easier to reach the point where re-linearization can be applied.

The number of invertible 8×8-matrices over $GF(2)$ is about $2^{62.2}$, and of these only about $2^{31.5}$ are linear over $GF(2^2)$. This means a random invertible $GF(2)$-matrix have a probability of less than 2^{-30} of being $GF(2^2)$-linear. A check has indeed verified that the matrix used in the S-box of Rijndael is not $GF(2^2)$-linear, and so the system can not be simplified this way. To our knowledge this is the first time it has been checked whether this matrix is linear over a larger field.

5 Conclusions

In this paper we have increased the list of ciphers dual to Rijndael from 240 to 9360. If this will have any impact on the security of Rijndael remains to be seen. Many properties of Rijndael, such as differential and linear probabilities, carry over to any of the duals, but other things can change. The designers of Rijndael stated in [2] that the constant b in the affine transformation of the S-box was chosen so the S-box would have no fixed points. However, some of the duals have an S-box with four fixed points.

The idea of describing one of the duals of Rijndael completely in terms of $GF(2^2)$ did not pay off this time, but we hope it could serve as an inspiration to do more algebraic analysis of the AES.

References

1. FIPS PUB 197. *Advanced Encryption Standard (AES)*, National Institute of Standards and Technology, U.S. Department of Commerce, November 2001. http://cscr.nist.gov/publications/fips/fips197/fips-197.pdf
2. J. Daemen, V. Rijmen. *AES Submission document on Rijndael, Version 2*, September 1999. http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf
3. N. Ferguson, R. Schroeppel, D. Whiting. *A Simple Algebraic Representation of Rijndael*. Selected Areas in Cryptography 2001, LNCS 2259, pp. 103-111, 2001.
4. S. Murphy, M. Robshaw. *Essential Algebraic Structure within the AES*. CRYPTO 2002, LNCS 2442, pp. 1-16, 2002
5. E. Barkan, E. Biham. *In How Many Ways Can You Write Rijndael?*. ASIACRYPT 2002, LNCS 2501, pp. 160-175, 2002.
6. N. Courtois, J. Pieprzyk. *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations*. ASIACRYPT 2002, LNCS 2501, pp. 267-287, 2002.
7. A. Biryukov, C. De Cannière, A. Braeken, B. Preneel. *A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms*. EUROCRYPT 2003, LNCS 2656, pp. 33-50, 2003.
8. J. Wolkerstorfer, E. Oswald, M. Lamberger. *An ASIC Implementation of the AES SBoxes*. CT-RSA 2002, LNCS 2271, pp. 67-78, 2002