Correlation Analysis in $\mathrm{GF}(2^n)$

Joan DAEMEN [a] and Vincent RIJMEN [b]
[a] *STMicroelectronics, Belgium*
[b] *Dept. of Electrical Engineering/ESAT, K.U.Leuven and IBBT and IAIK, Graz University of Technology, Austria*

Abstract. In this paper we provide a description of Rijndael using only algebraic operations in $\mathrm{GF}(2^8)$. How the elements of $\mathrm{GF}(2^8)$ are represented in bytes can be seen as a detail of the specification. In classical correlation analysis such as linear cryptanalysis, however, one works at the bit level and must assume a specific representation to study the propagation properties. We demonstrate how to conduct correlation analysis at the level of elements of $\mathrm{GF}(2^n)$, without having to deal with representation issues. While this approach does not result in better bounds or stronger attacks, it allows to analytically address the resistance against linear cryptanalysis similar to what has been done for differential cryptanalysis in [3]. Further we show how linear functions over $\mathrm{GF}(2)^n$ map one-to-one to linear functions over $\mathrm{GF}(2^n)$ by the choice of a basis, and make the link with their mask propagation properties.

Keywords. Linear cryptanalysis, Galois Fields, Correlation

Introduction

In the specification of Rijndael [2], we have extensively used operations in a finite field, where the bytes of the state and key represent elements of $\mathrm{GF}(2^8)$. Still, as for most block ciphers, Rijndael operates on plaintext blocks, ciphertext blocks and keys that are strings of bits. Apart from some exceptions such as interpolation attacks [5] and algebraically oriented analysis [4,8], cryptanalysis of ciphers is also generally conducted at the bit level. In particular, linear cryptanalysis exploits high correlations between linear combinations of bits of the state in different stages of the encryption process [2].

In Section 6, we demonstrate how Rijndael can be specified completely with algebraic operations in $\mathrm{GF}(2^8)$. How the elements of $\mathrm{GF}(2^8)$ are represented in bytes can be seen as a detail of the specification. Addressing this representation issue in the specifications is important for different implementations of Rijndael to be interoperable, but not more so than for instance the ordering of the bits within the bytes, or the way the bytes of the plaintext and ciphertext blocks are mapped onto the state bytes.

We can make abstraction from the representation of the elements of $\mathrm{GF}(2^8)$ and consider a block cipher that operates on strings of elements of $\mathrm{GF}(2^8)$. We call this generalisation RIJNDAEL-GF. Rijndael can be seen as an instance of RIJNDAEL-GF, where the representation of the elements has been specified. In principle, this can be applied to most block ciphers. Each block cipher for which the block length and the key length are a multiple of n can in principle be generalized to operate on strings of elements

of $\mathrm{GF}(2^n)$. However, unlike for Rijndael, the specification of these generalized ciphers may become quite complicated.

Intuitively, it seems obvious that if Rijndael has a cryptographic weakness, this is inherited by RIJNDAEL-GF and any instance of it, whatever the representation of the elements of $\mathrm{GF}(2^8)$. Still, in classical correlation analysis such as linear cryptanalysis one works at the bit level and must assume a specific representation to study the propagation properties. In this paper, we demonstrate how to conduct correlation analysis at the level of elements of $\mathrm{GF}(2^n)$, without having to deal with representation issues.

This paper is devoted to functions over fields with characteristic two. However, building on the generalization of linear cryptanalysis published in [1] all properties and theorems can be generalized to finite fields with odd characteristic. For clarity of description, we will denote the field $\mathrm{GF}(2)$ by $\mathbb{F}$ and a vector space over this field by $\mathbb{F}^n$. The extension field $\mathrm{GF}(2^n)$ will be denoted by $\mathbb{G}$ and a vector space over this extension field by $\mathbb{G}^\ell$.

We start by describing correlation properties of functions over $\mathbb{F}^n$ and of functions over $\mathbb{G}$, with the focus on linear functions. This is further generalized to functions over $\mathbb{G}^\ell$. We then discuss representations and bases in $\mathbb{F}^n$ and show how propagation in functions over $\mathbb{G}$ maps to propagation in vector Boolean functions by the choice of a basis. Subsequently, we prove two theorems that relate representations of linear functions in $\mathbb{F}^n$ and functions in $\mathbb{G}$ that are linear over $\mathbb{F}$. Finally we specify RIJNDAEL-GF.

1. Correlation in functions over $\mathbb{F}^n$

In this section we briefly recall some terms and definitions from 'standard' linear cryptanalysis.

We denote elements of $\mathbb{F}^n$ by $\boldsymbol{a}, \boldsymbol{b}$. The correlation between binary Boolean functions can be defined in terms of their Fourier counterparts $(-1)^{f(\boldsymbol{a})}$. Note that the Fourier counterpart of a Boolean function returns 1 if $f(\boldsymbol{a}) = 0$ and -1 if $f(\boldsymbol{a}) = 1$.

Definition 1 *The correlation $C_{f,g}$ between two binary Boolean functions $f(\boldsymbol{a})$ and $g(\boldsymbol{a})$ is defined as the expected value of the product of their Fourier counterparts:*

$$\begin{aligned} C_{f,g} &= \mathrm{E}\left[(-1)^{f(\boldsymbol{a})}(-1)^{g(\boldsymbol{a})}\right] \\ &= \mathrm{Prob}(f(\boldsymbol{a}) = g(\boldsymbol{a})) - \mathrm{Prob}(f(\boldsymbol{a}) \neq g(\boldsymbol{a})) \\ &= 2 \cdot \mathrm{Prob}(f(\boldsymbol{a}) = g(\boldsymbol{a})) - 1 \ . \end{aligned}$$

A *parity* of a Boolean vector is a binary Boolean function that consists of the binary sum (XOR) of a number of bits. A parity is determined by the positions of the bits of the Boolean vector that are included in the XOR.

The *(selection) mask* $\boldsymbol{w}$ of a parity is a Boolean vector value that has a 1 in the components that are included in the parity and a 0 in all other components. Analogous to the inner product of vectors in linear algebra, we express the parity of vector $\boldsymbol{a}$ corresponding with mask $\boldsymbol{w}$ as $\boldsymbol{w}^{\mathrm{T}}\boldsymbol{a}$. In this expression the T suffix denotes transposition of the vector $\boldsymbol{w}$.

In linear cryptanalysis, we need correlation between parities of input and output of a vector Boolean function $\boldsymbol{f}$. The correlation between input mask $\boldsymbol{w}$ and output mask $\boldsymbol{u}$ over a vector Boolean function $\boldsymbol{f}$ is given by:

$$\begin{aligned} C^{\boldsymbol{f}}_{\boldsymbol{u},\boldsymbol{w}} &= 2^{-n} \sum_{\boldsymbol{a}} (-1)^{\boldsymbol{w}^{\mathrm{T}}\boldsymbol{a}} (-1)^{\boldsymbol{u}^{\mathrm{T}}\boldsymbol{f}(\boldsymbol{a})} \\ &= 2^{-n} \sum_{\boldsymbol{a}} (-1)^{\boldsymbol{w}^{\mathrm{T}}\boldsymbol{a}+\boldsymbol{u}^{\mathrm{T}}\boldsymbol{f}(\boldsymbol{a})}. \end{aligned}$$

2. Description of correlation in functions over $\mathbb{G}$

In this section we study the correlation properties of the functions over $\mathbb{G}$:

$$f : \mathbb{G} \to \mathbb{G} : a \mapsto b = f(a).$$

All functions over $\mathbb{G}$ can be expressed as a polynomial over $\mathbb{G}$ of degree at most $2^n - 1$:

$$f(a) = \sum_{i=0}^{2^n-1} c_i a^i.$$

Given a table specification where the output value $f(a)$ is given for the 2^n different input values a, the 2^n coefficients of this polynomial can be found by applying Lagrange interpolation [7, p. 28]. On the other hand, given a polynomial expression, the table specification can be found by evaluating the polynomial for all values of a.

For Boolean functions, correlation is defined between parities. For a function over $\mathbb{G}$, individual bits cannot be distinguished without adopting a representation, and hence speaking about parities does not make sense. A parity is a function that maps $\mathbb{F}^n$ to $\mathbb{F}$, which is linear over $\mathbb{F}$. In $\mathbb{G}$, we can find functions with the same properties. For that purpose, we use the *trace* function in a finite field [7].

Definition 2 *Let x be an element of $\mathbb{G}$. The* trace *of x over $\mathbb{F}$ is defined by*

$$\mathrm{Tr}(x) = x + x^2 + x^{2^2} + x^{2^3} + \cdots + x^{2^{n-1}}.$$

The trace is linear over $\mathbb{F}$:

$$\begin{aligned} \forall\, x, y \in \mathbb{G} :\ & \mathrm{Tr}(x+y) = \mathrm{Tr}(x) + \mathrm{Tr}(y) \\ \forall\, a \in \mathbb{F}, \forall\, x \in \mathbb{G} :\ & \mathrm{Tr}(ax) = a\mathrm{Tr}(x). \end{aligned}$$

and it can be shown that $\mathrm{Tr}(x)$ is an element of $\mathbb{F}$.

It follows that the functions of the form

$$f(a) = \mathrm{Tr}(wa)$$

with $w \in \mathbb{G}$ are linear functions mapping $\mathbb{G}$ to $\mathbb{F}$. There are exactly 2^n such functions, one for each value of w. We call the function $\mathrm{Tr}(wa)$ a *trace parity*, and the corresponding value w a *trace mask*.

Example 1 *We consider the field* $\mathrm{GF}(2^3)$. *Let* α *be a root of* $x^3 + x + 1 = 0$. *Then the elements of* $\mathrm{GF}(2^3)$ *can be denoted by* $0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha$ *and* $\alpha^2+\alpha+1$. *The traces of the elements are given in Table 1.*

Table 1. The elements of $\mathrm{GF}(2^3)$ and their traces.

a	$\mathrm{Tr}(a)$	a	$\mathrm{Tr}(a)$
0	0	$\alpha^3 = \alpha + 1$	1
1	1	$\alpha^4 = \alpha^2 + \alpha$	0
α	0	$\alpha^5 = \alpha^2 + \alpha + 1$	1
α^2	0	$\alpha^6 = \alpha^2 + 1$	1

In the analysis of correlation properties of functions over $\mathbb{G}$, trace parities play the role that is played by the parities in the correlation analysis of Boolean functions, where $p = 2$ and $n = 1$. When a representation is chosen, these functions can be mapped one-to-one to parities (see Sect. 5.1).

By working with trace masks, it is possible to study correlation properties in functions over $\mathbb{G}$ without having to specify a basis. Hence, the obtained results are valid for all choices of basis. Once a basis is chosen, trace masks can be converted to selection masks (see Theorem 2).

For a function f over $\mathbb{G}$, we denote the correlation between an input trace parity $\mathrm{Tr}(wa)$ and an output trace parity $\mathrm{Tr}(uf(a))$ by $C^f_{u,w}$. We have

$$\begin{aligned} C^f_{u,w} &= 2^{-n} \sum_a (-1)^{\mathrm{Tr}(wa)} (-1)^{\mathrm{Tr}(uf(a))} \\ &= 2^{-n} \sum_a (-1)^{\mathrm{Tr}(wa)+\mathrm{Tr}(uf(a))} \\ &= 2^{-n} \sum_a (-1)^{\mathrm{Tr}(wa+uf(a))}. \end{aligned}$$

The value of this correlation is determined by the number of values a that satisfy

$$\mathrm{Tr}(wa + uf(a)) = 0. \tag{1}$$

If this equation is satisfied by r values a, the correlation $C^f_{u,w}$ is equal to $2^{1-n}r - 1$. If it has no solutions, the correlation is -1; if it is satisfied by all values a, the correlation is 1; and if it is satisfied by exactly half of the possible values a, the correlation is 0. By using the polynomial expression for f, (1) becomes a polynomial equation in a:

$$\mathrm{Tr}(wa + u \sum_i c_i a^i) = 0.$$

For some cases the number of solutions of these polynomials can be analytically determined providing provable bounds for correlation properties. See for example the results on Kloosterman sums in [6] that provide bounds on the input-output correlation of the multiplicative inverse in $\mathbb{G}$.

Example 2 *Let us consider the following operation:*

$$b = f(a) = a + \mathrm{c},$$

where c *is a constant. We can determine the correlation by finding the number of solutions of*

$$\mathrm{Tr}(wa + u(a + \mathrm{c})) = 0.$$

This is equivalent to

$$\mathrm{Tr}((w + u)a + u\mathrm{c}) = 0.$$

If $w + u$ *is different from 0, the trace is zero for exactly half of the values of* a*, and the correlation is 0. If* $w = u$ *this becomes*

$$\mathrm{Tr}(u\mathrm{c}) = 0.$$

This equation is true for all values of a *if* $\mathrm{Tr}(u\mathrm{c}) = 0$*, and has no solutions if* $\mathrm{Tr}(u\mathrm{c}) = 1$*. It follows that the addition of a constant has no effect on the trace mask and that the sign of the correlation is equal to* $(-1)^{\mathrm{Tr}(u\mathrm{c})}$.

2.1. Functions that are linear over $\mathbb{G}$

The functions of $\mathbb{G}$ that are linear over $\mathbb{G}$ are of the form

$$f(a) = l^{(0)}a,$$

where $l^{(0)}$ is an element of $\mathbb{G}$. Hence, there are exactly 2^n functions over $\mathbb{G}$ that are linear over $\mathbb{G}$.

For determining the correlation we can find the number of solutions of

$$\mathrm{Tr}(wa + ul^{(0)}a) = \mathrm{Tr}((w + ul^{(0)})a) = 0.$$

If the factor of a is different from 0, the correlation is 0. The correlation between $\mathrm{Tr}(wa)$ and $\mathrm{Tr}(ub)$ is equal to 1 iff

$$w = l^{(0)}u.$$

2.2. Functions that are linear over $\mathbb{F}$

A function over $\mathbb{G}$ is linear over $\mathbb{F}$ if it satisfies the following

$$\forall\, x, y \in \mathbb{G} : f(x + y) = f(x) + f(y)$$

Observe that the functions that are linear over $\mathbb{G}$ are a subset of the functions that are linear over $\mathbb{F}$. For example, the function $f(x) = x^2$ is linear over $\mathbb{F}$, but not over $\mathbb{G}$:

$$\begin{aligned} f(x + y) &= (x + y)^2 = x^2 + xy + yx + y^2 = x^2 + y^2 \\ &= f(x) + f(y) \\ f(ax) &= a^2 f(x) \neq af(x) \text{ if } a \notin \mathbb{F}. \end{aligned}$$

In general, the functions of $\mathbb{G}$ that are linear over $\mathbb{F}$ are the so-called linearized polynomials [7]:

$$f(a) = \sum_{t=0}^{n-1} l^{(t)} a^{2^t} \quad , \text{ with } l^{(t)} \in \mathbb{G}. \tag{2}$$

The relation between the trace mask at the input and the trace mask at the output is not trivial.

Theorem 1 *For a function $b = \sum_{t=0}^{n-1} l^{(t)} a^{2^t}$ an output trace parity $\mathrm{Tr}(ub)$ is correlated to input trace parity $\mathrm{Tr}(wa)$ with a correlation of 1 iff*

$$w = \sum_{t=0}^{n-1} (l^{(n-t \bmod n)} u)^{2^t}. \tag{3}$$

Proof 1 *We will prove that $\mathrm{Tr}(wa) = \mathrm{Tr}(ub)$ and hence that $\mathrm{Tr}(wa + ub) = 0$ for all values of a if w is given by (3). All computations with variables t, s and r are performed modulo n, and all summations are from 0 to $n-1$.*

$$\begin{aligned}
\mathrm{Tr}(wa) &= \mathrm{Tr}(ub) \\
\mathrm{Tr}\left(\sum_t (l^{(n-t)} u)^{2^t} a\right) &= \mathrm{Tr}\left(u \sum_t l^{(t)} a^{2^t}\right) \\
\sum_s \left(\sum_t {l^{(n-t)}}^{2^t} u^{2^t} a\right)^{2^s} &= \sum_s \left(\sum_t l^{(t)} u a^{2^t}\right)^{2^s} \\
\sum_s \sum_t {l^{(n-t)}}^{2^{s+t}} u^{2^{s+t}} a^{2^s} &= \sum_s \sum_t {l^{(t)}}^{2^s} u^{2^s} a^{2^{s+t}} \\
\sum_s \sum_t {l^{(n-t)}}^{2^{s+t}} u^{2^{s+t}} a^{2^s} &= \sum_{r=s+t} \sum_t {l^{(t)}}^{2^{r-t}} u^{2^{r-t}} a^{2^r} \\
\sum_s \sum_{r=n-t} {l^{(r)}}^{2^{s-r}} u^{2^{s-r}} a^{2^s} &= \sum_s \sum_t {l^{(t)}}^{2^{s-t}} u^{2^{s-t}} a^{2^s} \\
\sum_s \sum_t {l^{(t)}}^{2^{s-t}} u^{2^{s-t}} a^{2^s} &= \sum_s \sum_t {l^{(t)}}^{2^{s-t}} u^{2^{s-t}} a^{2^s}.
\end{aligned}$$

□

We illustrate this with the following example.

Example 3 *We consider two transformations f and g over $\mathrm{GF}(2^3)$, defined by*

$$f(a) = \alpha a$$
$$g(a) = a^4 + (\alpha^2 + \alpha + 1)a^2.$$

For both functions, we want to derive a general expression that for any output trace mask u gives the input trace mask w it correlates with. We denote these expressions by f_{d} and g_{d}, respectively. Applying Theorem 1, we obtain for $f(a)$:

$$l^{(0)} = \alpha,\ l^{(1)} = l^{(2)} = 0,$$

and hence

$$w = f_{\mathrm{d}}(u) = \alpha u. \tag{4}$$

Similarly, for $g(a)$ we have

$$l^{(0)} = 0,\ l^{(1)} = \alpha^2 + \alpha + 1,\ l^{(2)} = 1,$$

and hence

$$w = g_{\mathrm{d}} = u^2 + ((\alpha^2 + \alpha + 1)u)^4 = u^2 + (\alpha^2 + 1)u^4. \tag{5}$$

3. Description of correlation in functions over $\mathbb{G}^\ell$

In this section we treat the correlation properties of functions that operate on arrays of ℓ elements of $\mathbb{G}$. We denote the arrays by

$$\boldsymbol{A} = [a_1\ a_2\ a_3\ \ldots\ a_\ell\ ]^{\mathrm{T}}.$$

where the elements $a_i \in \mathbb{G}$. We have

$$Q : \mathbb{G}^\ell \to \mathbb{G}^\ell : \boldsymbol{A} \mapsto \boldsymbol{B} = F(\boldsymbol{A}).$$

The trace parities can be extended to vectors. We can define a trace mask vector as

$$\boldsymbol{W} = [w_1\ w_2\ w_3\ \ldots\ w_\ell]^{\mathrm{T}}.$$

where the elements $w_i \in \mathbb{G}$. The trace parities for a vector are of the form

$$\sum \mathrm{Tr}(w_i a_i) = \mathrm{Tr}\left(\sum_i w_i a_i\right) = \mathrm{Tr}(\boldsymbol{W}^{\mathrm{T}}\boldsymbol{A}).$$

We can define a correlation between an input trace parity $\mathrm{Tr}(\boldsymbol{W}^{\mathrm{T}}\boldsymbol{A})$ and an output trace parity $\mathrm{Tr}(\boldsymbol{U}^{\mathrm{T}}Q(\boldsymbol{A}))$:

$$\begin{aligned} C^F_{\boldsymbol{U},\boldsymbol{W}} &= 2^{-n\ell}\sum_{\boldsymbol{A}}(-1)^{\mathrm{Tr}(\boldsymbol{W}^{\mathrm{T}}\boldsymbol{A})}(-1)^{\mathrm{Tr}(\boldsymbol{U}^{\mathrm{T}}Q(\boldsymbol{A}))} \\ &= 2^{-n\ell}\sum_{\boldsymbol{A}}(-1)^{\mathrm{Tr}(\boldsymbol{W}^{\mathrm{T}}\boldsymbol{A})+\mathrm{Tr}(\boldsymbol{U}^{\mathrm{T}}Q(\boldsymbol{A}))} \\ &= 2^{-n\ell}\sum_{\boldsymbol{A}}(-1)^{\mathrm{Tr}(\boldsymbol{W}^{\mathrm{T}}\boldsymbol{A}+\boldsymbol{U}^{\mathrm{T}}Q(\boldsymbol{A}))}. \end{aligned}$$

3.1. Functions that are linear over $\mathbb{G}$

If F is linear over $\mathbb{G}$, it can be denoted by a matrix multiplication. We have

$$\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_\ell \end{bmatrix} = \begin{bmatrix} l_{1,1}\, l_{1,2}\, l_{1,3} \cdots l_{1,\ell} \\ l_{2,1}\, l_{2,2}\, l_{2,3} \cdots l_{2,\ell} \\ l_{3,1}\, l_{3,2}\, l_{3,3} \cdots l_{3,\ell} \\ \vdots \quad \vdots \quad \vdots \quad \ddots \quad \vdots \\ l_{\ell,1}\, l_{\ell,2}\, l_{\ell,3} \cdots l_{\ell,\ell} \end{bmatrix} \times \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_\ell \end{bmatrix}.$$

Or for short $\boldsymbol{B} = \mathsf{L}\boldsymbol{A}$. The elements of the matrix are elements of $\mathbb{G}$.

For the correlation, we have:

$$\begin{aligned} \mathrm{Tr}(\boldsymbol{W}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{U}^{\mathrm{T}}\mathsf{L}\boldsymbol{A}) &= \mathrm{Tr}(\boldsymbol{W}^{\mathrm{T}}\boldsymbol{A} + (\mathsf{L}^{\mathrm{T}}\boldsymbol{U})^{\mathrm{T}}\boldsymbol{A}) \\ &= \mathrm{Tr}((\boldsymbol{W} + \mathsf{L}^{\mathrm{T}}\boldsymbol{U})^{\mathrm{T}}\boldsymbol{A}). \end{aligned}$$

Hence, the correlation between $\mathrm{Tr}(\boldsymbol{W}^{\mathrm{T}}\boldsymbol{A})$ and $\mathrm{Tr}(\boldsymbol{U}^{\mathrm{T}}\boldsymbol{B})$ is equal to 1 if

$$\boldsymbol{W} = \mathsf{L}^{\mathrm{T}}\boldsymbol{U}. \tag{6}$$

3.2. Functions that are linear over $\mathbb{F}$

Generalizing equation (2) to vectors of $\mathbb{G}$ yields

$$b_i = \sum_j \sum_t l_{i,j}^{(t)} a_j^{2^t} \quad 0 \le i < n.$$

If we introduce the following notation:

$$\boldsymbol{A}^{2^t} = \left[a_1^{2^t}\ a_2^{2^t}\ a_3^{2^t}\ \ldots\ a_\ell^{2^t} \right],$$

this can be written as

$$\boldsymbol{B} = \sum_t \mathsf{L}^{(t)} \boldsymbol{A}^{2^t}.$$

For the relation between the input trace mask and the output trace mask, it can be proven that

$$\boldsymbol{W} = \sum_t (\mathsf{L}^{(n-t \bmod n)^{\mathrm{T}}} \boldsymbol{U})^{2^t}.$$

4. Representations of $\mathbb{G}$

In this section we treat vector representations of $\mathbb{G}$, bases and dual bases. These play an essential role in the mapping of propagation properties from functions over $\mathbb{G}$ to those of Boolean functions.

4.1. Vector space representation of $\mathbb{G}$

The additive group of the finite field $\mathbb{G}$ and the n-dimensional vector space over $\mathbb{F}$ are isomorphic. The addition of vectors in this vector space corresponds to the addition in $\mathbb{G}$. We can choose a basis e consisting of n elements $e^{(i)} \in \mathbb{G}$. We depict the basis e by a column vector that has as elements the elements of the basis:

$$\mathsf{e} = \left[e^{(1)} \; e^{(2)} \; \cdots \; e^{(n)} \right]^{\mathrm{T}}$$

The elements of $\mathbb{G}$ can be represented by their coordinates with respect to this basis. We have

$$a = \sum_i a_i e^{(i)} = \boldsymbol{a}^{\mathrm{T}} \mathsf{e}. \tag{7}$$

where $a_i \in \mathbb{F}$ are the coordinates of a with respect to the basis e and where $\boldsymbol{a}$ is the column vector consisting of coordinates a_i. The map

$$\phi_{\mathsf{e}} : \mathbb{G} \to \mathbb{F}^n : a \mapsto \phi_{\mathsf{e}}(a) = \boldsymbol{a}$$

forms an isomorphism.

4.2. Dual Bases

Coordinates of a field element with respect to a basis can be expressed in terms of the *dual basis* and the *trace* map.

Definition 3 *Two bases* e *and* d *are called* dual bases *if for all* i *and* j *with* $1 \leq i$ *and* $j \leq n$*, it holds that*

$$\mathrm{Tr}(d^{(i)} e^{(j)}) = \delta(i \oplus j), \tag{8}$$

Every base has exactly one dual base. Let e and d be dual bases. Then we have

$$\mathrm{Tr}(d^{(j)} a) = \mathrm{Tr}\left(d^{(j)} \sum_{i=1}^{n} a_i e^{(i)} \right) = \sum_{i=1}^{n} a_i \mathrm{Tr}(d^{(j)} e^{(i)}) = a_j.$$

Hence the coordinates with respect to basis e can be expressed in an elegant way by means of the trace map and the dual basis d [7]:

$$\phi_{\mathsf{e}}(a) = \boldsymbol{a} = \left[\mathrm{Tr}(d^{(1)} a) \; \mathrm{Tr}(d^{(2)} a) \; \ldots \; \mathrm{Tr}(d^{(n)} a) \right]. \tag{9}$$

Applying (7) gives:

$$a = \sum_{i=1}^{n} \mathrm{Tr}(d^{(i)} a) e^{(i)} = \sum_{i=1}^{n} \mathrm{Tr}(e^{(i)} a) d^{(i)}. \tag{10}$$

Example 4 *By choosing a basis, we can represent the elements of* $\mathrm{GF}(2^3)$ *as vectors. We choose the basis* e *as follows:*

$$\mathsf{e} = [\alpha^2 + \alpha + 1, \alpha + 1, 1]^{\mathrm{T}}.$$

The dual basis of e *can be determined by solving (8). It is given by*

$$\mathsf{d} = [\alpha, \alpha^2 + \alpha, \alpha^2 + 1]^{\mathrm{T}}.$$

Table 2 shows the coordinates of the elements of $\mathrm{GF}(2^3)$*, with respect to both bases.*

Table 2. Coordinates of the field elements, with respect to the bases e and d.

a	$\boldsymbol{a}$	$\boldsymbol{a}_{\mathrm{d}}$
0	000	000
1	001	111
$\alpha + 1$	010	011
α	011	100
$\alpha^2 + \alpha + 1$	100	101
$\alpha^2 + \alpha$	101	010
α^2	110	110
$\alpha^2 + 1$	111	001

5. Boolean Functions and Functions in $\mathbb{G}$

Functions of $\mathbb{G}$ can be mapped to functions of $\mathbb{F}^n$ by choosing a basis e in $\mathbb{G}$. Given

$$f : \mathbb{G} \to \mathbb{G} : a \mapsto b = f(a),$$

we can define a vector Boolean function $\boldsymbol{f}$:

$$\boldsymbol{f} : \mathbb{F}^n \to \mathbb{F}^n : \boldsymbol{a} \mapsto \boldsymbol{b} = \boldsymbol{f}(\boldsymbol{a})$$

where

$$\boldsymbol{a} = [a_1\ a_2\ \ldots\ a_n]$$
$$\boldsymbol{b} = [b_1\ b_2\ \ldots\ b_n],$$

and

$$a_i = \mathrm{Tr}(ad^{(i)})$$
$$b_i = \mathrm{Tr}(bd^{(i)}).$$

On the other hand, given a vector Boolean function $\boldsymbol{g}$, a function over $\mathbb{G}$ can be defined as

$$a = \boldsymbol{a}^{\mathrm{T}}\mathsf{e}$$
$$b = \boldsymbol{b}^{\mathrm{T}}\mathsf{e}.$$

So in short, $\boldsymbol{f} = \phi_{\mathsf{e}} \circ f \circ \phi_{\mathsf{e}}^{-1}$ and $f = \phi_{\mathsf{e}}^{-1} \circ \boldsymbol{f} \circ \phi_{\mathsf{e}}$.

This can be extended to functions operating on vectors of elements of $\mathbb{G}$.

5.1. Relationship Between Trace Masks and Selection Masks

If we study correlations in $\mathbb{F}^n$, then we have to use selection masks, and we need to specify a basis. We can avoid specification of a basis if we study instead the correlations in $\mathbb{G}$, and work with trace masks. Since there exists an isomorphism between $\mathbb{F}^n$ and $\mathbb{G}$, we can expect that for every selection mask $\boldsymbol{w}$ there exists a trace mask w, and vice versa.

Since generally $\mathrm{Tr}(wa) \neq \phi_{\mathsf{e}}(w)^{\mathrm{T}}\boldsymbol{a}$, a selection mask $\boldsymbol{w} = \phi_{\mathsf{e}}(w)$ usually does not correspond to the trace mask w. This is illustrated by the example below.

Example 5 *We use basis* e *defined in Example 4. We take* $w = \alpha$*, hence* $\boldsymbol{w}^{\mathrm{T}} = [011]$*. Then it follows from Table 3 that* $\mathrm{Tr}(wa) \neq \boldsymbol{w}^{\mathrm{T}}\boldsymbol{a}$*.*

Table 3. $\mathrm{Tr}(wa) \neq \boldsymbol{w}^{\mathrm{T}}\boldsymbol{a}$.

a	$\boldsymbol{a}^{\mathrm{T}}$	$\mathrm{Tr}(\alpha a)$	$[011]^{\mathrm{T}}\boldsymbol{a}$
0	000	0	0
1	001	0	1
$\alpha+1$	010	0	1
α	011	0	0
$\alpha^2+\alpha+1$	100	1	0
$\alpha^2+\alpha$	101	1	1
α^2	110	1	1
α^2+1	111	1	0

In the following theorem, we give and prove the correct relation between trace masks and selection masks.

Theorem 2 *Let* $\boldsymbol{a} = \phi_{\mathsf{e}}(a)$*. Then the trace mask* w *corresponds to* $\phi_{\mathsf{d}}(w)$ *with* d *the dual basis of* e*.*

Proof 2 *We prove that*

$$\mathrm{Tr}(wa) = \boldsymbol{w}_{\mathrm{d}}{}^{\mathrm{T}}\boldsymbol{a},$$

and hence that the correlations in $\mathbb{F}^n$ *and* $\mathbb{G}$ *have the same value if the relation between the masks is satisfied. Applying (10) to* w *and* a*, we get*

$$\mathrm{Tr}(wa) = \mathrm{Tr}\left(\left(\sum_i \mathrm{Tr}(e^{(i)}w)d^{(i)}\right)\left(\sum_j \mathrm{Tr}(d^{(j)}a)e^{(j)}\right)\right).$$

Since the output of the trace map lies in $\mathbb{F}$*, and since the trace map is linear over* $\mathbb{F}$*, we can convert this to:*

$$\begin{aligned}\mathrm{Tr}(wa) &= \sum_i \mathrm{Tr}(e^{(i)}w)\sum_j \mathrm{Tr}(d^{(j)}a)\mathrm{Tr}(d^{(i)}e^{(j)})\\ &= \sum_i \mathrm{Tr}(e^{(i)}w)\sum_j \mathrm{Tr}(d^{(j)}a)\delta(i\oplus j)\\ &= \sum_i \mathrm{Tr}(e^{(i)}w)\mathrm{Tr}(d^{(i)}a).\end{aligned}$$

Applying (9) twice completes the proof. □

5.2. Relationship Between Linear Functions in $\mathbb{F}^n$ and $\mathbb{G}$

A linear function of $\mathbb{F}^n$ is completely specified by an $n \times n$ matrix M:

$$\boldsymbol{b} = \mathsf{M}\boldsymbol{a}.$$

A linear function of $\mathbb{G}$ is specified by the n coefficients $l^{(t)} \in \mathbb{G}$ in

$$b = \sum_{t=0}^{n-1} l^{(t)} a^{2^t}.$$

After choosing a basis e over $\mathbb{G}$, these two representations can be converted to one another.

Theorem 3 *Given the coefficients $l^{(t)}$ and a basis e, the elements of the matrix M are given by*

$$M_{ij} = \sum_{t=0}^{n-1} \mathrm{Tr}\left(l^{(t)} d^{(i)} {e^{(j)}}^{2^t}\right).$$

Proof 3 *We will derive an expression of b_i as a linear combination of a_j in terms of the factors $l^{(t)}$. For a component b_i we have*

$$\begin{aligned} b_i &= \mathrm{Tr}(b d^{(i)}) \\ &= \mathrm{Tr}\left(\sum_t l^{(t)} a^{2^t} d^{(i)}\right) \\ &= \sum_t \mathrm{Tr}(l^{(t)} a^{2^t} d^{(i)}). \end{aligned} \tag{11}$$

The powers of a can be expressed in terms of the components a_j:

$$\begin{aligned} a^{2^t} &= \left(\sum_j a_j e^{(j)}\right)^{2^t} \\ &= \sum_j a_j {e^{(j)}}^{2^t}, \end{aligned} \tag{12}$$

where we use the fact that exponentiation by 2^t is linear over $\mathbb{F}$ to obtain (12). Substituting (12) in (11) yields

$$\begin{aligned} b_i &= \sum_t \mathrm{Tr}\left(l^{(t)} \sum_j a_j {e^{(j)}}^{2^t} d^{(i)}\right) \\ &= \sum_t \sum_j \mathrm{Tr}\left(l^{(t)} {e^{(j)}}^{2^t} d^{(i)} a_j\right) \end{aligned}$$

$$= \sum_j \left(\sum_t \mathrm{Tr}(l^{(t)} {e^{(j)}}^{2^t} d^{(i)}) \right) a_j.$$

It follows that

$$M_{ij} = \sum_t \mathrm{Tr} \left(l^{(t)} {e^{(j)}}^{2^t} d^{(i)} \right),$$

proving the theorem. □

Theorem 4 *Given matrix* M *and a basis* e*, the elements* $l^{(t)}$ *are given by*

$$l^{(t)} = \sum_{i=1}^{n} \sum_{j=1}^{n} M_{ij} {d^{(j)}}^{2^t} e^{(i)}.$$

Proof 4 *We will express* b *as a function of powers of* a *in terms of the elements of the matrix* M*. We have*

$$b = \sum_i b_i e^{(i)}, \tag{13}$$

and

$$\begin{aligned} b_i &= \sum_j M_{ij} a_j \\ &= \sum_j M_{ij} \mathrm{Tr}(a d^{(j)}) \\ &= \sum_j M_{ij} \sum_t a^{2^t} {d^{(j)}}^{2^t}. \end{aligned} \tag{14}$$

Substituting (14) into (13) yields

$$\begin{aligned} b &= \sum_i \sum_j M_{ij} \sum_t a^{2^t} {d^{(j)}}^{2^t} e^{(i)} \\ &= \sum_t \left(\sum_i \sum_j M_{ij} {d^{(j)}}^{2^t} e^{(i)} \right) a^{2^t}. \end{aligned}$$

It follows that

$$l^{(t)} = \sum_i \sum_j M_{ij} {d^{(j)}}^{2^t} e^{(i)},$$

proving the theorem. □

Figure 1 illustrates the relations between the selection mask and trace mask at the input and output of linear functions in $\mathbb{G}$. Remember that we always express the *input* mask w as a function of the *output* mask u.

We illustrate this in the next example.

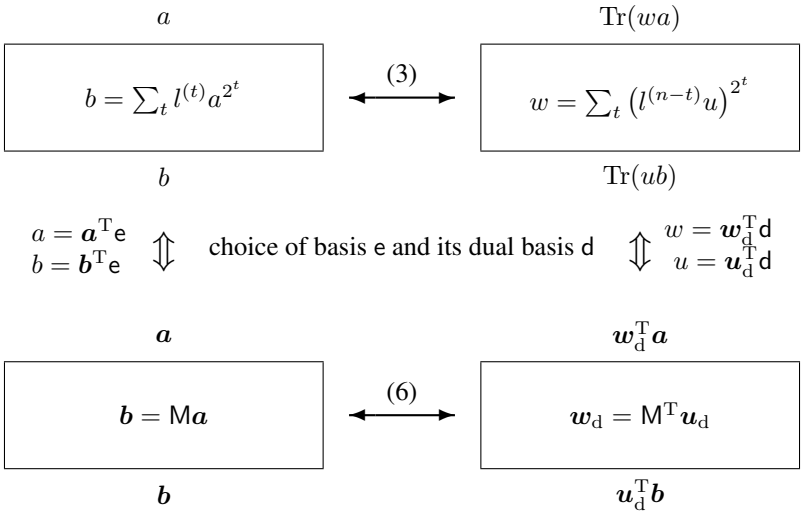

Figure 1. The propagation of selection and trace masks through a function that is linear over $\mathbb{F}$.

Example 6 *We take the functions f and g of Example 3 and the bases* e *and* d *of Example 4. Table 4 shows the coordinates of the elements of* $\mathrm{GF}(2^3)$*, as well as the coordinates of the images of f and g with respect to* e*.*

Table 4. Coordinates of the field elements, and the images of f and g with respect to the basis e.

a	$\boldsymbol{a}$	$\boldsymbol{b} = f(a)$	$\boldsymbol{b} = g(a)$
0	000	000	000
1	001	011	101
$\alpha + 1$	010	101	001
α	011	110	100
$\alpha^2 + \alpha + 1$	100	111	100
$\alpha^2 + \alpha$	101	100	001
α^2	110	010	101
$\alpha^2 + 1$	111	001	000

Once the coordinates of the inputs and outputs of f and g have been determined, we can derive the matrices M *and* N *that describe the functions $\boldsymbol{f}$ and $\boldsymbol{g}$ in the vector space:*

$$\mathsf{M} = \begin{bmatrix} 1\,1\,0 \\ 1\,0\,1 \\ 1\,1\,1 \end{bmatrix} \quad , \quad \mathsf{N} = \begin{bmatrix} 1\,0\,1 \\ 0\,0\,0 \\ 0\,1\,1 \end{bmatrix} .$$

The transformations to derive input selection masks from output selection masks are determined by M^{T} *and* N^{T}*:*

$$\boldsymbol{f}_{\mathrm{d}}(\boldsymbol{u}_{\mathrm{d}}) = \mathsf{M}^{\mathrm{T}}\boldsymbol{u}_{\mathrm{d}} \tag{15}$$

$$\boldsymbol{g}_{\mathrm{d}}(\boldsymbol{u}_{\mathrm{d}}) = \mathsf{N}^{\mathrm{T}}\boldsymbol{u}_{\mathrm{d}}. \tag{16}$$

Table 5 shows for all the elements of $\mathrm{GF}(2^3)$ *the coordinates with respect to basis* d *in the first column, the coordinates of the images of* $\boldsymbol{f}_\mathrm{d}$ *and* $\boldsymbol{g}_\mathrm{d}$ *calculated according to (15) and (16) and the second and third column. The fourth column gives the elements of* $\mathrm{GF}(2^3)$*, the fifth and the sixth column give the functions* f *and* g *according to (4)–(5). It can now be verified that the coordinates in the second, respectively the third column correspond to the field elements in the fifth, respectively the sixth column.*

Table 5. The functions f_d and g_d.

$\boldsymbol{u}_\mathrm{d}$	$\boldsymbol{w}_\mathrm{d} = \boldsymbol{f}_\mathrm{d}(\boldsymbol{u}_\mathrm{d})$	$\boldsymbol{w}_\mathrm{d} = \boldsymbol{g}_\mathrm{d}(\boldsymbol{u}_\mathrm{d})$	u	$w = f_\mathrm{d}(u)$	$w = g_\mathrm{d}(u)$
000	000	000	0	0	0
001	111	011	α^2+1	1	$\alpha+1$
010	101	000	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0
011	010	011	$\alpha+1$	$\alpha^2+\alpha$	$\alpha+1$
100	110	101	α	α^2	$\alpha^2+\alpha+1$
101	001	110	$\alpha^2+\alpha+1$	α^2+1	α^2
110	011	101	α^2	$\alpha+1$	$\alpha^2+\alpha+1$
111	100	110	1	α	α^2

6. Rijndael-GF

We will now define RIJNDAEL-GF. This is a block cipher very much like Rijndael, but in which the keys, plaintext and ciphertexts consist of sequences of elements of $\mathrm{GF}(2^8)$ rather than bytes. We will express constants in this specification by powers of α, where α is a root of the primitive polynomial $x^8+x^4+x^3+x^2+1$ and hence a generator of the multiplicative group of $\mathrm{GF}(2^8)$.

We will first specify the RIJNDAEL-GF round transformation. It operates on a state in $\mathrm{GF}(2^8)^n_\mathrm{t}$ where $n_\mathrm{t} \in \{16, 20, 24, 28, 32\}$.

The step `SubBytes-GF` operates on the individual elements of the state. It is composed of two sub-steps. The first step is taking the multiplicative inverse in $\mathbb{G}$:

$$g(a) = a^{-1}, \tag{17}$$

with 0 mapping to 0. The second sub-step consists of applying the following linearized polynomial:

$$f(a) = \alpha^2 a + \alpha^{199} a^{2} + \alpha^{99} a^{2^2} + \alpha^{185} a^{2^3} + \alpha^{197} a^{2^4} + a^{2^5} + \alpha^{96} a^{2^6} + \alpha^{232} a^{2^7}, \tag{18}$$

followed by the addition of the following constant: α^{195}.

The step `ShiftRows-GF` is a transposition that does not modify the values of the elements in the state but merely changes their positions. It is the same as in Rijndael.

The mixing step `MixColumns-GF` operates independently on 4-element columns and mixes them linearly by multiplication with the following matrix:

$$\begin{bmatrix} \alpha^{25} & \alpha & 1 & 1 \\ 1 & \alpha^{25} & \alpha & 1 \\ 1 & 1 & \alpha^{25} & \alpha \\ \alpha & 1 & 1 & \alpha^{25} \end{bmatrix}$$

Finally, the addition of a round key `AddRoundKey-GF` consists of the addition of a round key by a simple addition in $\mathrm{GF}(2^8)$.

The key expansion is the same as that in Rijndael, with the exception that the Rijndael S-boxes are replaced by the RIJNDAEL-GF S-box and the round constants defined as $\mathrm{RC}[i] = \alpha^{25(i-1)}$.

RIJNDAEL-GF, together with the choice of a representation of the elements of $\mathrm{GF}(2^8)$ as bytes constitutes a block cipher operating on bit strings. We can now show that RIJNDAEL-GF is equivalent to Rijndael. As a matter of fact, the choice of the following basis converts RIJNDAEL-GF into Rijndael:

$$\mathsf{e} = 1, \alpha^{25}, \alpha^{50}, \alpha^{75}, \alpha^{100}, \alpha^{125}, \alpha^{150}, \alpha^{175}.$$

We can compute the corresponding dual basis d by solving (8). This yields:

$$\mathsf{d} = \alpha^{166}, \alpha^{187}, \alpha^{37}, \alpha^{26}, \alpha^{236}, \alpha^{191}, \alpha^{196}, \alpha^{48}.$$

In Rijndael the second sub-step of the S-box is specified as the multiplication with a binary matrix. This matrix can be reconstructed by applying Theorem 3 to (18) using these bases. The equivalence of the matrices of `MixColumns` and `MixColumns-GF` follows from the fact that $\phi_{\mathsf{e}}^{-1}(\mathtt{02}) = \alpha^{25}$ and $\phi_{\mathsf{e}}^{-1}(\mathtt{03}) = 1 + \alpha^{25} = \alpha$.

References

[1] Thomas Baignères, Jacques Stern, and Serge Vaudenay, *Linear cryptanalysis of non binary ciphers*, Selected Areas in Cryptography (Carlisle M. Adams, Ali Miri, and Michael J. Wiener, eds.), Lecture Notes in Computer Science, vol. 4876, Springer, 2007, pp. 184–211.

[2] J. Daemen and V. Rijmen, *The design of Rijndael — AES, the advanced encryption standard*, Springer-Verlag, 2002.

[3] Joan Daemen and Vincent Rijmen, *Understanding two-round differentials in aes*, SCN (Roberto De Prisco and Moti Yung, eds.), Lecture Notes in Computer Science, vol. 4116, Springer, 2006, pp. 78–94.

[4] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David Wagner, and Doug Whiting, *Improved cryptanalysis of Rijndael*, FSE (Bruce Schneier, ed.), Lecture Notes in Computer Science, vol. 1978, Springer, 2000, pp. 213–230.

[5] Thomas Jakobsen and Lars R. Knudsen, *The interpolation attack on block ciphers*, FSE (Eli Biham, ed.), Lecture Notes in Computer Science, vol. 1267, Springer, 1997, pp. 28–40.

[6] Gilles Lachaud and Jacques Wolfmann, *The weights of the orthogonals of the extended quadratic binary Goppa codes*, IEEE Transactions on Information Theory **36** (1990), no. 3, 686–692.

[7] Rudolf Lidl and Harald Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1986 (Reprinted 1988).

[8] Sean Murphy and Matthew J. B. Robshaw, *Essential algebraic structure within the AES*, CRYPTO (Moti Yung, ed.), Lecture Notes in Computer Science, vol. 2442, Springer, 2002, pp. 1–16.