12. Correlation Analysis in GF(2^n)

This chapter is based on Appendix A of the first edition of this book and [52]. In the specification of Rijndael in Chap. 3, we have extensively used operations in a finite field, where the bytes of the state and key represent elements of 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 [73] and algebraically oriented analysis [61, 115], 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; see Chap. 7. Differential cryptanalysis (see Chap. 8) exploits high propagation probabilities between bitwise differences in the state in different stages of the encryption.

In Section 12.4, we demonstrate how Rijndael can be specified completely with algebraic operations in GF(2^8). How the elements of GF(2^8) are represented in bytes can be seen as a detail of the specification. Addressing this representation issue in the specification 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 abstract away from the representation of the elements of GF(2^8) and consider a block cipher that operates on strings of elements of GF(2^8). We call this generalization 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 with block length and key length that are a multiple of n can in principle be generalized to operate on strings of elements of 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 GF(2^8). Still, in the correlation analysis as described in Chap. 7, we work at the bit level and must assume a specific representation to study the propagation properties. In this chapter, we

J. Daemen, V. Rijmen, *The Design of Rijndael*, Information Security and Cryptography,
https://doi.org/10.1007/978-3-662-60769-5_12

demonstrate how to conduct correlation analysis at the level of elements of GF(2^n), without having to deal with representation issues.

This chapter is devoted to functions over fields with characteristic two. However, building on the generalization of linear cryptanalysis published in [8] all properties and theorems can be generalized to finite fields with odd characteristic.

We start by describing correlation properties of functions over $\mathrm{GF}(2)^n$ and of functions over GF(2^n), with the focus on linear functions. This is further generalized to functions over $\mathrm{GF}(2^n)^\ell$. We then discuss representations and bases in $\mathrm{GF}(2)^n$ and show how propagation in functions over GF(2^n) maps to propagation in Boolean functions by the choice of a basis. Subsequently, we prove two theorems that relate representations of linear functions in $\mathrm{GF}(2)^n$ and functions in GF(2^n) that are linear over GF(2). Finally we specify Rijndael-GF.

12.1 Description of Correlation in Functions over GF(2^n)

In this section we study the correlation properties of the functions over GF(2^n):

$$f : \mathrm{GF}(2^n) \to \mathrm{GF}(2^n) : a \mapsto b = f(a).$$

For Boolean functions, correlation is defined between parities. For a function over GF(2^n), 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 $\mathrm{GF}(2)^n$ to GF(2) and is linear over GF(2). In GF(2^n), we can find functions with the same properties. For that purpose, we use the *trace* function in a finite field (see Section 2.1.8).

It follows that the functions of the form

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

with $w \in \mathrm{GF}(2^n)$ are linear functions mapping GF(2^n) to GF(2). 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*.

In the analysis of correlation properties of functions over GF(2^n), trace parities play the role that is played by the parities in the correlation analysis of Boolean functions, where $n = 1$. When a representation is chosen, these functions can be mapped one-to-one to parities (see Sect. 12.3.1).

By working with trace masks, it is possible to study correlation properties in functions over GF(2^n) 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 the usual masks, which we will call *selection masks* in this chapter (see Theorem 12.3.1).

For a function f over GF(2^n), we denote the correlation between an input trace parity $\mathrm{Tr}(wa)$ and an output trace parity $\mathrm{Tr}(uf(a))$ by $\mathsf{C}_{u,w}^{(f)}$. We have

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

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

$$\mathrm{Tr}(wa + uf(a)) = 0. \tag{12.1}$$

If this equation is satisfied by r such values, the correlation $\mathsf{C}_{u,w}^{(f)}$ 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, (12.1) becomes a polynomial equation in a (see Section 2.1.8):

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

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 [92] that provide bounds on the input-output correlation of the multiplicative inverse in GF(2^n).

Example 12.1.1. 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

$$\mathrm{Tr}(uc) = 0.$$

This equation is true for all values of a if $\mathrm{Tr}(uc) = 0$, and has no solutions if $\mathrm{Tr}(uc) = 1$. 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 $(-1)^{\mathrm{Tr}(uc)}$.

12.1.1 Functions That Are Linear over GF(2^n)

The functions of GF(2^n) that are linear over GF(2^n) (see Sect. 2.1.2) are of the form

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

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

To determine 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 $\mathrm{Tr}(uf(a))$ is equal to 1 iff

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

12.1.2 Functions That Are Linear over GF(2)

A function over GF(2^n) is linear over GF(2) if it satisfies the following:

$$\forall\ x, y \in \mathrm{GF}(2^n) : f(x + y) = f(x) + f(y)\ .$$

Observe that the functions that are linear over GF(2^n) are a subset of the functions that are linear over GF(2). For example, the function $f(x) = x^2$ is linear over GF(2), but not over GF(2^n):

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

In general, the functions of GF(2^n) that are linear over GF(2) are the so-called linearized polynomials [95]:

$$f(a) = \sum_{t=0}^{n-1} l^{(t)} a^{2^t}\ ,\ \text{with } l^{(t)} \in \mathrm{GF}(2^n). \tag{12.2}$$

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

Theorem 12.1.1. *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*

$$w = \sum_{t=0}^{n-1} (l^{(n-t \bmod n)} u)^{2^t}. \tag{12.3}$$

Proof. 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 (12.3). 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 12.1.2. We consider two transformations f and g over GF(2^3), defined by

$$\begin{aligned}
f(a) &= \alpha a \\
g(a) &= a^4 + (\alpha^2 + \alpha + 1) a^2.
\end{aligned}$$

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 12.1.1, we obtain for $f(a)$

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

and hence

$$w = f_{\mathrm{d}}(u) = \alpha u. \tag{12.4}$$

Similarly, for $g(a)$ we have

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

and hence

$$w = g_{\mathrm{d}} = u^2 + ((\alpha^2 + \alpha + 1)u)^4 = u^2 + (\alpha^2 + 1)u^4. \tag{12.5}$$

12.2 Description of Correlation in Functions over $\mathbf{GF}(\mathbf{2^n})^{\boldsymbol{\ell}}$

In this section we treat the correlation properties of functions that operate on arrays of ℓ elements of GF(2^n). We denote the arrays by

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

where the elements $a_i \in \mathrm{GF}(2^n)$. We have

$$Q : \mathrm{GF}(2^n)^\ell \to \mathrm{GF}(2^n)^\ell : \mathbf{A} \mapsto \mathbf{B} = F(\mathbf{A}).$$

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

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

where the elements $w_i \in \mathrm{GF}(2^n)$. The trace parities for a vector are of the form

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

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

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

12.2.1 Functions That Are Linear over GF(2^n)

If F is linear over GF(2^n), it can be denoted by a matrix multiplication. We have

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

Or for short $\mathbf{B} = \mathsf{L}\mathbf{A}$. The elements of the matrix are elements of GF(2^n).

For the correlation, we have

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

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

$$\mathbf{W} = \mathsf{L}^{\mathrm{T}}\mathbf{U}. \tag{12.6}$$

12.2.2 Functions That Are Linear over GF(2)

Generalizing equation (12.2) to vectors of GF(2^n) 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:

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

this can be written as

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

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

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

12.3 Boolean Functions and Functions in GF(2^n)

12.3.1 Relationship Between Trace Masks and Selection Masks

If we study correlations in GF$(2)^n$, 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 GF(2^n), and work with trace masks. Since there exists an isomorphism between GF$(2)^n$ and GF(2^n), 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 $\boldsymbol{w} = \phi_{\mathsf{e}}(w)$, with ϕ defined in Sect. 2.1.9, usually does not correspond to the trace mask w. This is illustrated by the example below.

Example 12.3.1. We use basis e defined in Example 2.1.10. We take $w = \alpha$, hence $\boldsymbol{w}^{\mathrm{T}} = [011]$. Then it follows from Table 12.1 that $\mathrm{Tr}(wa) \neq \boldsymbol{w}^{\mathrm{T}}\boldsymbol{a}$.

Table 12.1. $\mathrm{Tr}(wa) \neq \boldsymbol{w}^{\mathrm{T}}\boldsymbol{a}$

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

Proof. We prove that

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

and hence that the correlations in GF$(2)^n$ and GF(2^n) have the same value if the relation between the masks is satisfied. Applying (2.42) 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 GF(2), and since the trace map is linear over GF(2), 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 (2.41) twice completes the proof. □

12.3.2 Relationship Between Linear Functions in GF(2)^n and GF(2^n)

A linear function of GF(2)^n is completely specified by an $n \times n$ matrix M:

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

A linear function of GF(2^n) is specified by the n coefficients $l^{(t)} \in \mathrm{GF}(2^n)$ in

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

After choosing a basis e over GF(2^n), these two representations can be converted to one another.

Theorem 12.3.2. *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. 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

$$\begin{aligned}b_i &= \mathrm{Tr}(bd^{(i)}) \\ &= \mathrm{Tr}\left(\sum_t l^{(t)} a^{2^t} d^{(i)}\right) \\ &= \sum_t \mathrm{Tr}(l^{(t)} a^{2^t} d^{(i)}).\end{aligned} \tag{12.7}$$

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

$$a^{2^t} = \left(\sum_j a_j e^{(j)}\right)^{2^t}$$
$$= \sum_j a_j {e^{(j)}}^{2^t}, \tag{12.8}$$

where we use the fact that exponentiation by 2^t is linear over GF(2) to obtain (12.8). Substituting (12.8) in (12.7) yields

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

It follows that

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

proving the theorem. □

Theorem 12.3.3. *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. We will express b as a function of powers of a in terms of the elements of the matrix M. We have

$$b = \sum_i b_i e^{(i)}, \tag{12.9}$$

and

$$b_i = \sum_j M_{ij} a_j$$
$$= \sum_j M_{ij} \mathrm{Tr}(a d^{(j)})$$
$$= \sum_j M_{ij} \sum_t a^{2^t} {d^{(j)}}^{2^t}. \tag{12.10}$$

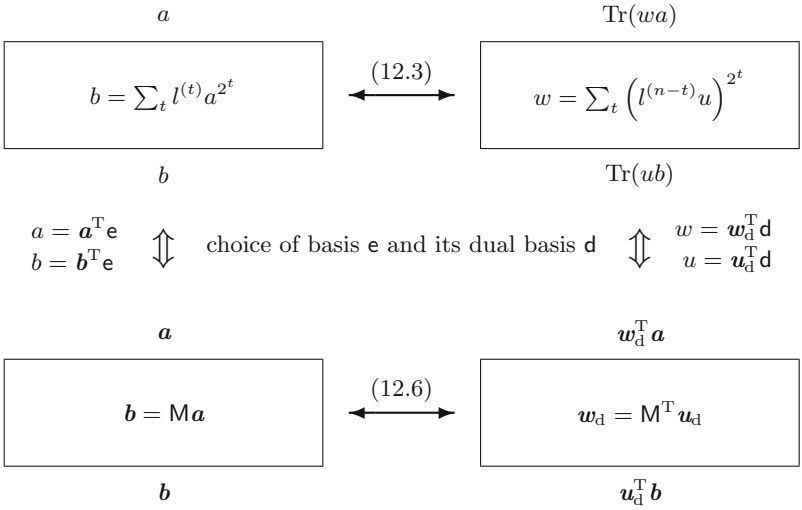

Fig. 12.1. The propagation of selection and trace masks through a function that is linear over GF(2)

Substituting (12.10) into (12.9) 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 12.1 illustrates the relations between the selection mask and trace mask at the input and output of linear functions in GF(2^n). Remember that we always express the *input* mask w as a function of the *output* mask u.

We illustrate this in the next example.

Example 12.3.2. We take the functions f and g of Example 12.1.2 and the bases e and d of Example 2.1.10. Table 12.2 shows the coordinates of the elements of GF(2^3), as well as the coordinates of the images of f and g with respect to e.

Table 12.2. 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:

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

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

$$\boldsymbol{f}_{\mathrm{d}}(\boldsymbol{u}_{\mathrm{d}}) = \mathsf{M}^{\mathrm{T}}\boldsymbol{u}_{\mathrm{d}} \tag{12.11}$$

$$\boldsymbol{g}_{\mathrm{d}}(\boldsymbol{u}_{\mathrm{d}}) = \mathsf{N}^{\mathrm{T}}\boldsymbol{u}_{\mathrm{d}}. \tag{12.12}$$

Table 12.3 shows for all the elements of GF(2^3) the coordinates with respect to basis d in the first column, and the coordinates of the images of $\boldsymbol{f}_{\mathrm{d}}$ and $\boldsymbol{g}_{\mathrm{d}}$ calculated according to (12.11) and (12.12) in the second and third column. The fourth column gives the elements of GF(2^3), the fifth and the sixth column give the functions f and g according to (12.4)–(12.5). 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.

12.4 Rijndael-GF

We will now define Rijndael-GF. This is a block cipher very much like Rijndael, but with keys, plaintext and ciphertexts that consist of sequences of elements of 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 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 $n_{\mathrm{t}} \in \{16, 20, 24, 28, 32\}$.

Table 12.3. 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

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 GF(2^n):

$$g(a) = a^{-1}, \tag{12.13}$$

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

$$f(a) = \alpha^2 a + \alpha^{199} a^2 + \alpha^{99} a^{2^2} + \alpha^{185} a^{2^3} + \alpha^{197} a^{2^4} + a^{2^5} + \alpha^{96} a^{2^6} + \alpha^{232} a^{2^7}, \tag{12.14}$$

followed by the addition of the 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 four-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 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 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:

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

We can compute the corresponding dual basis d by solving (2.40). This yields:

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

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 12.3.2 to (12.14) 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 $\phi_{\mathsf{e}}^{-1}(\mathtt{03}) = 1 + \alpha^{25} = \alpha$.