# An Algebraic Framework for Cipher Embeddings

C. Cid[1]*, S. Murphy[1], and M.J.B. Robshaw[2]

[1]Information Security Group,
Royal Holloway, University of London,
Egham, Surrey, TW20 0EX, U.K.

[2]France Télécom Research and Development
38–40 rue du Général-Leclerc,
92794 Issy les Moulineaux, France

**Abstract.** In this paper we discuss the idea of block cipher embeddings and consider a natural algebraic framework for such constructions. In this approach we regard block cipher state spaces as algebras and study some properties of cipher extensions on larger algebras. We apply this framework to some well-known examples of AES embeddings.

## 1 Introduction

Cryptosystems are designed to hinder the efforts of the cryptanalyst. However it is good cryptographic practice to ensure that the cryptosystem is presented in a clear and natural manner to facilitate independent scrutiny. Since there is rarely one single viewpoint for looking at a cipher, one approach for the cryptanalyst is to consider alternative presentations. At first sight it may appear that there is little to be gained by studying the same cryptosystem in a different way. However, new perspectives may well:

- reveal mathematical structure that was hidden;
- permit calculations that were previously considered intractable;
- encourage the development of ideas about the analysis of the cryptosystem;
- provide implementation insights.

In fact, finding different presentations is fundamentally the only technique available for the analysis of many asymmetric cryptosystems, as the following two examples of widely used asymmetric cryptosystems demonstrate.

- **RSA.** The security of the RSA cryptosystem [16] with modulus $n$, where $n = pq$ (two unknown primes), is believed to fundamentally depend on the inability of an attacker to factor the integer $n$. This is equivalent to the inability of an attacker to find a presentation based on the ring "factoring" isomorphism $\mathbb{Z}_n \to \mathbb{Z}_p \times \mathbb{Z}_q$.

* This author was supported by EPSRC Grant GR/S42637.

- **Cryptosystems based on Discrete Logarithms.** There are many cryptosystems, such as ElGamal [5], the Digital Signature Standard [15] or Elliptic Curves [10, 7], whose security is believed to fundamentally depend on the inability of an attacker to calculate discrete logarithms in certain finite cyclic groups. For such a group $G$ of order $p$, this is equivalent to the inability of an attacker to find a presentation based on the isomorphism $G \to \mathbb{Z}_p^+$, where $\mathbb{Z}_p^+$ is the additive cyclic group of integers modulo $p$.

For an asymmetric cryptosystem, it is often fairly obvious which presentation of the cryptosystem might be of greatest use to the analyst. The difficulty for an alternative presentation of an asymmetric cryptosystem is "merely" one of calculating this presentation.

For a symmetric cryptosystem it is unlikely to be so obvious. One standard technique for analysing a mathematical structure is to *embed* it as a sub-structure within a larger one. In this way the original mathematical structure is presented within the context of a larger structure and such an approach has yielded great insights in many areas of mathematics. In this paper, therefore, we consider a framework for the embeddings of block ciphers.

While embeddings are usually constructed in the hope that they can provide a further insight to the cryptanalyst, they can also be useful when considering some implementation issues: an alternative presentation could provide a more efficient implementation of the cipher, or might be used to protect against some forms of side-channel attacks, such as timing or power analysis.

Our discussion is conducted with a view to providing a basic framework for block cipher embeddings. The question of whether a particular block cipher embedding yields any new insights might be, to some extent, a subjective judgement. However we observe that there are embeddings that are in some sense "trivial" and they cannot possibly offer extra insight into the cipher. In this paper we seek to provide a framework to provide some initial discrimination between embeddings of different types.

We begin the development of this framework by considering the natural mathematical structure for a block cipher state space, namely the algebra. The embedding of one block cipher into a larger one is then discussed in terms of the embedding function between the two state space algebras. This leads to a natural mathematical derivation of the extended cryptographic functions of the larger block cipher. To illustrate our approach, we discuss some well-known examples of AES embeddings [1, 11, 12].

## 2 State Space Algebras

The state space of a block cipher is usually composed of a number of identical components. For example, the state space of the Data Encryption Standard (DES) [13] consists of 64 bits, whereas the state space of the Advanced Encryption Standard (AES) [14, 3, 4] is usually thought of as consisting of 16 bytes. For many block ciphers, these components are viewed as elements of some algebraic structure, and internal block cipher computations often depend on using operations based on this structure. Thus, it is natural to regard a component of the DES state space as an element of the finite field $GF(2)$, and a component of the AES state space as an element of the field $GF(2^8)$.

For a block cipher, in which a component of the state space is naturally regarded as an element of a field $K$, the entire state space is given by the set $K^n$, where $n$ is the number of components ($n = 64$ for the DES and $n = 16$ for the AES). The set $K^n$ has a natural ring structure as the direct sum of $n$ copies of the field $K$, as well as a natural vector space structure as a vector space of dimension $n$ over $K$. A set with such structure is known as an *algebra* [8]. More formally, we have the following definition.

**Definition 1.** *Let $K$ be a field. An associative* $K$**-algebra** *(or simply* algebra*) is a vector space $A$ over $K$ equipped with an associative $K$-bilinear multiplication operation.*

Informally, we can regard an algebra as a vector space which is also a ring. Algebras can be also generalised to the case when $K$ is a commutative ring (in which case $A$ is a $K$-module rather than a vector space). The dimension of the algebra $A$ is the dimension of $A$ as a vector space. The set $A' \subset A$ is a subalgebra of $A$ if $A'$ is an algebra in its own right, and $A'$ is an ideal subalgebra if it is also an ideal of the ring $A$. We can also classify mappings between two algebras in the obvious way, so an algebra homomorphism is a mapping that is both a ring homomorphism and a vector space homomorphism (linear transformation).

Considering block ciphers, the algebra of most interest cryptographically is formed by the set $K^n$. This is an algebra of dimension $n$ over $K$, where "scalar" multiplication by the field element $\lambda \in K$ is identified with multiplication by the ring element $(\lambda, \ldots, \lambda) \in K^n$. This algebra is the natural algebraic structure for most block cipher state spaces and we term the algebra $K^n$ the *state space algebra*. We note that even in cases where $K$ is not a field (for example, a component of the state space of the SAFER family of block ciphers [9] is most naturally thought of as an element of the ring $\mathbb{Z}_{2^8}$), the $K$-algebra $K^n$ still remains the most interesting structure for our analysis, and most of the discussion following can be suitably modified.

The algebraic transformations of a state space algebra, that is transformations that preserve most of the structure of the algebra, are necessarily based either on a linear transformation of the state space or on a ring-based transformation of the state space. However, a secure design often requires some non-algebraic block cipher transformations; for example in each round there is often a transformation using a substitution or look-up table. There are cases however (most notably the AES) where the round transformations are dominated by algebraic operations and, in such cases, it may be interesting to study the cipher by means of an embedding of the state space algebra in a larger algebra. An embedding may be defined so that all transformations of the embedded state space are also algebraic transformations with respect to the larger algebra. The hope is that this new representation may offer new insights on the essential structure of the original cipher.

## 3 Block Cipher Embeddings

Suppose that $A = K^n$ is the state space algebra of dimension $n$ over $K$ for some block cipher, and that the encryption process consists of a family of (key-dependent) functions $f : A \to A$. A block cipher embedding is constructed from an injective mapping $\eta : A \to B$ from the algebra $A$ into some (possibly larger) algebra $B$ and suitably extended versions of the functions $f$ defined on $B$. We now consider different methods of embedding block ciphers.

### 3.1 Identity Embeddings

The are clearly many ways of embedding $A$ in an algebra $B$ of higher dimension. One obviously unproductive way to construct a cipher embedding is to embed the algebra $A$ and the cryptographic function $f$ into the algebra $B$ by means of the *identity* mapping.

Suppose that the algebra $B$ can be written as the direct sum

$$B = A \oplus A',$$

with the embedding mapping given by $\eta : a \mapsto (a, 0)$. The functions $f$ can easily be extended in a trivial manner, so that $(a, 0) \mapsto (f(a), 0)$. This provides a direct mirror of the cipher within $B$, and the $A'$-component of the embedding (and the value of the extended function beyond $\eta(A)$) is irrelevant to the definition of the original cipher in its embedded form. Clearly, this idea can also be extended to any embedding mapping of the form $\eta : a \mapsto (a, ?)$ and any extension of $f$ to a function $(a, ?) \mapsto (f(a), ?)$. For example, the cryptographic function $f : A \to A$ could be extended to a cryptographic function $\widehat{f} : B \to B$ given by $(a, a') \mapsto (f(a), g(a'))$ for some function $g : A' \to A'$.

Knudsen essentially gives an example of such an embedding where $f$ is the Data Encryption Standard (DES) [13] encryption function and $g$ is the RSA [16] encryption function, with the same key used (in very different ways) for each of these encryption functions [6]. Based on this embedding function, Knudsen makes statements about the security of DES in terms of the security of RSA and vice versa [6]. The readers of [6] are left to draw their own conclusions about a security statement made about one cipher but which is based on the analysis of a different arbitrary cipher.

We term such an embedding an *identity-reducible* embedding. Apart from possibly providing another presentation of the cipher, identity-reducible embeddings are of little interest mathematically or cryptographically.

### 3.2 Induced Embeddings

The starting point for a cipher embedding is an injective function $\eta : A \to B$. We denote by $B_A = \eta(A) \subset B$ the image of this mapping. We now discuss the natural method of extending the cipher functions $f$ to functions on $B$ using $\eta$.

We first consider how to define the induced embedded cryptographic functions $f_\eta : B_A \rightarrow B_A$. These functions need to mirror the action of $f$ on $A$, but within $B_A$. They must therefore be given by

$$f_\eta(b) = \eta\left(f\left(\eta^{-1}\left(b\right)\right)\right) \text{ for } b \in B_A,$$

which is illustrated in the diagram below (Figure 1). To illustrate this induced function, consider the usual case where subkeys are introduced into a block cipher by addition, that is by the function $f(a) = a + k$. Suppose we choose an additive embedding transformation $\eta$, whose definition can be extended to subkeys. In this case, the corresponding embedded method of introducing subkeys can be naturally defined by addition, as

$$\begin{tikzcd}
A \arrow[d] & B_A \arrow[l, "\eta^{-1}"'] \arrow[d] \\
\boxed{f} \arrow[d] & \boxed{f_\eta} \arrow[d] \\
A \arrow[r, "\eta"] & B_A
\end{tikzcd}$$

**Fig. 1.** Induced Function given by the Embedding $\eta$.

$$f_\eta\left(\eta(a)\right) = \eta\left(f\left(\eta^{-1}\left(\eta(a)\right)\right)\right) = \eta\left(f(a)\right) = \eta(a+k) = \eta(a) + \eta(k).$$

### 3.3 Natural Extensions of Embeddings

The reason for considering an embedding is to analyse a cipher within a (possibly) larger cipher in the hope of gaining a better insight into the original cipher. In general however, $B_A = \eta(A)$ is not a subalgebra of $B$, but it exists within the context of the algebra $B$ and operations on $B_A$ are defined by the algebra $B$. It is thus far more natural to work within the algebra $B$ and define $B_A$ mathematically within $B$, than it is to consider $B_A$ in isolation. For example, while $B_A$ may not be a vector space, the induced encryption functions may be defined in terms of a matrix multiplication of the elements of $B_A$. It is clearly mathematically appropriate in such an example to consider the vector space on which the linear transformation is defined instead of just one subset (e.g. $B_A$). It is thus desirable in an embedding to *naturally* extend the function $f_\eta$ to $B$, so that the extension retains the main algebraic properties of $f_\eta$.

The most appropriate structure to consider in this case would be the set $\overline{B}_A$, the (algebraic) *closure* of $B_A$. This is the minimal algebra containing $B_A$, and is generated (as an algebra) by the elements of $B_A$. The set $B_A$ can now be considered algebraically entirely within the context of the closure $\overline{B}_A$, and the operations on $B_A$ are defined within the algebra $\overline{B}_A$.

It is clear how this notion of closure can give the appropriate extension of the induced functions $f_\eta : B_A \to B_A$ to an extended induced functions $\overline{f}_\eta : \overline{B}_A \to \overline{B}_A$. In particular, such an extension $\overline{f}_\eta$ preserves algebraic relationships between the input and output of the functions $f_\eta$. It should also be clear that $\overline{B}_A$ is the absolute extent of the cipher within $B$. No elements outside $\overline{B}_A$ (that is $B \setminus \overline{B}_A$) can be generated by the embedded versions of elements of the state space algebra $A$. Thus the extension of any function beyond $\overline{B}_A$ is not determined algebraically by the original cipher function, and can thus be considered arbitrary. There seems to be no need (or point) in considering anything beyond the closure of the embedding.

We have thus described a natural three-step process for embedding a cipher within another cipher with a larger state space algebra:

1. Define an injective embedding function from the original state space algebra to the larger state space algebra.
2. Based on the embedding function, define the induced cryptographic functions on the embedded image of the original state space algebra.
3. Extend these induced cryptographic functions in a *natural* manner to the larger state space algebra by algebraic closure.

This general approach seems to be an appropriate framework for considering cipher embeddings, particularly for ciphers with a highly algebraic structure (note that key schedules can usually be similarly embedded). However it is clear that each embedding should be considered on its own merits. Furthermore, not every property of the embedded cipher is of immediate relevance to the original cipher. Indeed, an example of a weakness of the larger algebraically embedded cipher that does not translate to the original cipher was given in [12]. However our framework allows us to immediately identify some embeddings that inevitably have little cryptanalytical value.

## 4 Embeddings of the AES

The AES [14] is a cipher with a highly algebraic structure, and it is a suitable cipher on which to apply and analyse different embedding methods. We look at three different approaches that have been proposed in the literature and consider their merits in terms of the framework given in Section 3.

The AES encryption process is typically described using operations on an array of bytes, which we can regard as an element of the field $\mathbb{F} = GF(2^8)$. Without loss of generality, we consider the version of the AES with 16-byte message and key spaces, and 10 encryption rounds. The state space algebra of the AES is thus the algebra $\mathbb{F}^{16}$, which we denote by $\mathbf{A}$.

### 4.1 Dual Ciphers of the AES

In [1] Barkan and Biham construct a number of alternative representations of the AES, which they call *dual ciphers* of Rijndael. These distinct representations are derived from the automorphisms of the finite field $\mathbb{F} = GF(2^8)$ (based on the Fröbenius map $a \mapsto a^2$) and the different representations of the field itself (via the explicit isomorphisms between fields of order $2^8$). Each representation can clearly be seen as a form of embedding; the embedding functions are isomorphisms and therefore $B \cong A$. The AES cryptographic functions are extended to $B$ according to these isomorphisms. These embeddings are essentially mirrors of the AES, although the different representations may permit us to gain a better insight of algebraic structure of the cipher, such as the importance of some of the choices made in the design of the AES. For instance, by analysing different representations, it is concluded that a change of the "Rijndael polynomial" (used to represent the finite field $GF(2^8)$ within the cipher) should not affect the strength of the cipher [1]. Such alternative representations can also be useful in providing additional insights into efficient and secure implementation practices.

### 4.2 The BES Extension of the AES

The embedding of the AES in a larger cipher called Big Encryption System (BES) was introduced in [12]. The main goal of this construction was to represent the AES within a framework where the cipher could be expressed through simple operations (inversion and affine transformation) in the field $\mathbb{F} = GF(2^8)$.

The BES operates on 128-byte blocks with 128-byte keys and has a very simple algebraic structure. The state space algebra of the AES is the algebra $\mathbf{A} = \mathbb{F}^{16}$, while the state space algebra of the BES is the algebra $\mathbb{F}^{128}$ (denoted by $\mathbf{B}$). The embedding function for the BES embedding is based on the vector conjugate mapping $\phi : \mathbb{F} \to \mathbb{F}^8$ [12], which maps an element of $\mathbb{F}$ to a vector of its eight conjugates. Thus $\phi$ is an injective ring homomorphism given by

$$\phi(a) = \left(a^{2^0}, a^{2^1}, a^{2^2}, a^{2^3}, a^{2^4}, a^{2^5}, a^{2^6}, a^{2^7}\right).$$

This definition can be extended in the obvious way to an embedding function $\phi : \mathbf{A} \to \mathbf{B}$ given by $\phi(\mathbf{a}) = \phi(a_0, \ldots, a_{15}) = (\phi(a_0), \ldots, \phi(a_{15}))$, which is an injective ring homomorphism. We note that the image of this ring homomorphism, $\mathbf{B}_A = Im(\phi)$, is a subring of $\mathbf{B}$, but not a subalgebra. However, it contains a basis for $\mathbf{B}$ as a vector space, and so $\mathbf{B}$ is the closure of $\mathbf{B}_A$. Thus $\phi$ is not a identity-reducible embedding.

The three-step process of Section 3 shows how this embedding gives an embedded cipher on $\mathbf{B}$. Based on the embedding function $\phi$, an encryption function $f : \mathbf{A} \to \mathbf{A}$ of the AES induces an embedded encryption function $f_\phi : \mathbf{B}_A \to \mathbf{B}_A$. This can be naturally extended by closure to a function $\overline{f}_\phi : \mathbf{B} \to \mathbf{B}$. This extension to $\mathbf{B}$ can be expressed by simple operations over $GF(2^8)$, namely inversion and affine transformation. These are natural extensions of the algebraic operations of the AES to the larger algebra $\mathbf{B}$, based on the embedding function.

The AES embedding in the BES is an example of a cipher embedding which yields insights into the cipher that are not apparent from the original description. This is demonstrated by the multivariate quadratic equation system for the AES that is based on the BES embedding [12, 2], which is a much simpler multivariate quadratic equation system than can be obtained directly from the AES. More generally, it is clear that the AES embedding in the BES offers a more natural environment in which to study the algebraic properties of the AES.

### 4.3 AES Extensions of Monnerat and Vaudenay

Monnerat and Vaudenay recently considered extensions of the AES and the BES, namely the CES and the Big-BES [11]. The authors showed that these were *weak* extensions in which cryptanalytic attacks could be easily mounted. They observed however that the weaknesses in the larger ciphers did not translate to weaknesses in the AES and BES, and were therefore of no consequence to the security of the AES. Within the framework established in Section 3 it is now very easy to see why the extensions given in [11] are inevitably divorced from the original cipher.

The extensions of the AES to CES and the Big-BES are similar, so we only consider the extension of the AES to the CES in this paper. A component of the state space for the CES can be considered as an element of the set $\mathbf{R} = \mathbb{F} \times \mathbb{F}$. The set $\mathbf{R}$ is given a ring structure $(\mathbf{R}, \oplus, \otimes)$ with binary operations defined by:

$$\begin{array}{ll} \text{Addition} & (x_1, y_1) \oplus (x_2, y_2) = \ (x_1 + x_2\ ,\ y_1 + y_2)\,, \\ \text{Multiplication} & (x_1, y_1) \otimes (x_2, y_2) = (x_1 x_2\ ,\ x_1 y_2 + x_2 y_1)\,. \end{array}$$

The state space algebra for the CES is the algebra $\mathbf{C} = \mathbf{R}^{16}$, which is an algebra of dimension 32 over $\mathbb{F}$, with scalar multiplication by the field element $\lambda \in \mathbb{F}$ being identified with multiplication by the ring element $(\lambda, 0, \lambda, 0, \ldots, \lambda, 0) \in \mathbf{C}$.

The embedding of the AES in the CES is based on the injective algebra homomorphism $\theta : \mathbb{F} \to \mathbf{R}$ given by $\theta(a) = (a, 0)$. This definition can be extended in the obvious way to the injective algebra homomorphism $\theta : \mathbf{A} \to \mathbf{C}$

$$\theta\,(\mathbf{a}) = \theta\,(a_0, \ldots, a_{15}) = (\theta(a_0), \ldots, \theta(a_{15})) = ((a_0, 0), \ldots, (a_{15}, 0))\,.$$

The AES cryptographic functions were then induced based on this embedding map, and extended to the entire state space $\mathbf{C}$ to define the cipher CES.

There are several reasons why the cryptographic and algebraic relevance of such an embedding would be immediately questionable. Firstly, the definition of the function on the embedded image does not appear to be appropriate since some important algebraic properties are not retained within the CES. For instance, the AES "inversion" function satisfies $x^{(-1)} = x^{254}$, but this algebraic relationship is not satisfied by the CES "inversion" function. Secondly, the algebra $\mathbf{C}$ can be expressed as the direct sum of $\mathbf{C}_A = Im(\theta)$ and some other ideal subalgebra $\mathbf{C}'$. Thus, in our terminology, $\theta$ is a identity-reducible embedding. As shown earlier, this means that the way the embedded encryption function $f_\theta : \mathbf{C}_A \to \mathbf{C}_A$ is extended beyond $\mathbf{C}_A$ is irrelevant and has no consequences in the analysis of the AES. However, the cryptanalysis of the CES given in [11] is based on the properties of this arbitrary $\mathbf{C}'$-component of the CES. The fundamental reason for this separation into two components is clearly seen using the framework presented in this paper. The other embedding mappings proposed in [11] (based on $a \mapsto (a, \lambda a)$) are also identity-reducible and so at a fundamental level they are bound to have the same ineffectiveness in tying together the properties of the underlying cipher and the extension cipher.

# 5 Regular Representations of State Space Algebras

A very powerful and widely used technique in the study of algebras is to embed an algebra in a matrix algebra. Such an embedding of an algebra is known as a *representation* of the algebra. Thus a representation of a state space algebra gives an embedding of a cipher in a matrix algebra. In this section, we consider how a cipher state space algebra may be represented as matrix algebra, and how such a matrix representation can highlight properties of the cipher and its state space.

A *representation* of an $n$-dimensional algebra $A$ is formally defined as an algebra homomorphism from $A$ to a subalgebra of $M_l(K)$ [8], where $M_l(K)$ denotes the set of $l \times l$ matrices over the field $K$. Thus a representation of the algebra $A$ identifies $A$ with an $n$-dimensional subalgebra of the $l \times l$ matrices. If the algebra homomorphism is an isomorphism, then we may identify $A$ with this $n$-dimensional subalgebra of the $l \times l$ matrices. Clearly, there are many ways in to define a representation. One standard technique is the *regular* representation, which is the algebra homomorphism $\nu : A \to M_n(K)$ that maps $a \in A$ to the matrix corresponding to the linear transformation $z \mapsto az$ ($z$ a $K$-vector of length $n$) [8].

An illustration of a regular representation is given by the complex numbers, which form a 2-dimensional algebra over the real numbers. The complex number $x+iy$ can be identified with its regular representation as a matrix, which is given by

$$\nu(x+iy) = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}.$$

The set of all such matrices forms a 2-dimensional algebra over the real numbers and can be identified with the complex numbers.

## 5.1 Regular Representation of the AES and the BES

The regular representations of the AES and the BES state spaces are algebra homomorphisms to diagonal matrix algebras. Thus we identify elements of these state spaces with the obvious diagonal matrix. An element of the AES state space $\mathbf{A}$ has a regular representation as a $16 \times 16$ diagonal matrix over $\mathbb{F}$, so $\mathbf{A}$ can be thought of as the $16 \times 16$ diagonal matrices. An embedded element of the AES state space in the BES has a regular representation as a diagonal $128 \times 128$ matrix over $\mathbb{F}$ in which the diagonal consists of octets of conjugates. The closure under matrix (algebra) operations of such embedded elements is clearly the algebra of all $128 \times 128$ diagonal matrices, which is the regular representation of the state space algebra $\mathbf{B}$. The BES, and hence the AES, can thus be defined in terms of standard matrix operations in the regular representation of $\mathbf{B}$. Suppose $B$ is the diagonal $128 \times 128$ matrix that is the regular representation of some $\mathbf{b} \in \mathbf{B}$, then these BES transformations are given in matrix terms below.

- **Inversion**. For diagonal matrix $B$, this is the mapping $B \mapsto B^{(-1)} = B^{254}$. For an invertible diagonal matrix $B$, this is matrix inversion.
- **Linear Diffusion**. For diagonal matrix $B$, there exist diagonal matrices $D_i$ and permutation matrices $P_i$ $(i = 0, \ldots, 31)$ such that this linear transformation can be defined by
$$B \mapsto \sum_{i=0}^{31} D_i P_i B P_i^T .$$
- **Subkey Addition.** For diagonal matrix $B$ and round subkey diagonal matrix $K$, this is the mapping $B \mapsto B + K$.

Thus the BES can be defined in matrix terms through the regular representation of the algebra $\mathbf{B}$ as the subalgebra of diagonal matrices, with the operations of the BES being represented by algebraic operations on these matrices.

The natural algebraic method of generalising operations on diagonal matrices is to extend these operations by some method to a larger algebra of matrices that contain the diagonal matrices. Thus we could define a "Matrix-AES" or "Matrix-BES" defined on some algebra of matrices that coincides with the AES or the BES for diagonal matrices. As we discuss below, this is in fact the approach taken in [11] to give the definition of the CES and the Big-BES. However, the functional "inversion" operation $M \mapsto M^{254}$ is not an invertible mapping on any subalgebra containing non-diagonal matrices. Thus there is no algebraic extension of the AES or BES state spaces beyond the diagonal matrices. In any case, the regular representation of the AES and the BES state spaces as diagonal matrices illustrates very well the point made in Section 3. From the viewpoint of the AES or the BES, all extensions beyond diagonal matrices are arbitrary and algebraically indistinguishable.

### 5.2 Regular Representations of Monnerat–Vaudenay Embeddings

We now consider the regular representation corresponding to the Monnerat and Vaudenay embedding. The algebra $R$ has dimension 2 over $\mathbb{F}$, so its regular representation is given by a 2-dimensional subalgebra of the $2 \times 2$ matrices over $\mathbb{F}$. For an element $(x, y) \in \mathbf{R}$, the regular representation (with right matrix multiplication) is given by
$$\nu\left((x, y)\right) = \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} .$$

Thus the regular representation of $R$ is as the algebra of triangular matrices with constant diagonals, with the subalgebra corresponding to the embedding of $\mathbb{F}$ in $\mathbf{R}$ being the 1-dimensional subalgebra of $2 \times 2$ diagonal matrices with constant diagonals. It is clear that in any matrix operation related to the AES, the value of the diagonal elements never depends on any off-diagonal element. The regular representation of the CES state space ($\mathbf{C}$) is a subalgebra of the $32 \times 32$ matrices over $\mathbb{F}$ given by the 32-dimensional subalgebra of $2 \times 2$ block diagonal matrices of the form given above. The regular representation of the AES subalgebra of the CES is given by the 16-dimensional subalgebra of diagonal matrices with pairs of constant terms. As noted above, the off-diagonal elements never have any effect on the diagonal elements and are entirely arbitrary. However, from the algebraic viewpoint of the AES, this subalgebra of diagonal matrices is the only subalgebra with any relevance. We note that this subalgebra of diagonal matrices is a representation in the $32 \times 32$ matrices of the algebra $\mathbf{A}$, and is clearly algebra isomorphic to the subalgebra of diagonal $16 \times 16$ matrices, which is the regular representation of the AES state space $\mathbf{A}$.

All the regular representations of the AES subset of the various state spaces considered consist of diagonal matrices. Those diagonal matrices given by the regular representation of Monnerat and Vaudenay embeddings merely use diagonal matrices of twice the size with diagonal entries repeated. Every cipher considered (AES, BES, CES and Big-BES) can all be defined solely in matrix terms within the subalgebra of diagonal matrices. Any extension of the block cipher definitions beyond diagonal matrices is arbitrary. The use of other embeddings based on similar algebraic structures is also suggested in [11]. However, it can be seen that the regular representations of the state space algebras of such embeddings merely correspond to other matrix subalgebras containing the diagonal matrix subalgebra. Thus such other embeddings also have the same cryptographic relevance as the original embeddings of Monnerat and Vaudenay [11]. Any conclusions drawn about diagonal matrices (AES embeddings) by considering the effect of these arbitrary block ciphers on non-diagonal matrices is arbitrary.

## 6 Conclusions

In this paper, we have presented a natural framework for the analysis of block cipher embeddings. This has been done in terms of the algebra of their state spaces, but takes into consideration the construction of the embedding function, how to "naturally" induce the cryptographic function on the embedded image, and how to (possibly) extend this image to the algebraic closure.

In this way we have shown that different approaches to embeddings in the literature are not algebraically equivalent. By way of example we have looked at three embedding strategies that have been discussed in the context of the AES. It is clear that while some embeddings might bring benefits such as cryptanalytic or implementation insights, it is possible to define other embeddings that, by their very construction, cannot possibly offer additional insights into the cipher.

## References

1. E. Barkan and E. Biham. In How Many Ways Can You Write Rijndael?. *ASIACRYPT 2002*, LNCS vol. 2501, pp 160–175, Springer, 2002.
2. C. Cid, S. Murphy, and M.J.B. Robshaw. Computational and Algebraic Aspects of the Advanced Encryption Standard. In V. Ganzha *et al.*, editors, Proceedings of the *Seventh International Workshop on Computer Algebra in Scientific Computing - CASC 2004*, St. Petersburg, Russia, pages 93–103, Technische Universität München". 2004.
3. J. Daemen and V. Rijmen. AES Proposal: Rijndael (Version 2). NIST AES website `csrc.nist.gov/encryption/aes`, 1999.
4. J. Daemen and V. Rijmen. *The Design of Rijndael: AES—The Advanced Encryption Standard*. Springer–Verlag, 2002.
5. T. ElGamal. A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms. *IEEE Transactions on Information Theory*, vol. 31, pp. 469–472, 1985.
6. L.R. Knudsen. New Directions in Cryptography (Volume II). *Journal of Craptology*, available at `http://www2.mat.dtu.dk/people/Lars.R.Knudsen/crap.html`, Vol. 1 No. 0, December 2000.
7. N. Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, Vol. 48, pp 321-348, 1987.
8. A.I. Kostrikin. *Introduction to Algebra*. Springer-Verlag, 1981.
9. J.L. Massey. SAFER K-64: A byte-oriented block-ciphering algorithm. *Fast Software Encryption 1993*, LNCS vol. 809, pp. 1–17, Springer-Verlag, 1994.
10. V.S. Miller. Uses of Elliptic Curves in Cryptography. *CRYPTO '85*, LNCS vol. 218, pp. 417-426, Springer-Verlag, 1986.
11. J. Monnerat and S. Vaudenay. On some Weak Extensions of AES and BES. *Sixth International Conference on Information and Communications Security 2004*, LNCS vol. 3269, pp414–426, Springer, 2004.
12. S. Murphy and M.J.B. Robshaw. Essential Algebraic Structure within the AES. *CRYPTO 2002*, LNCS vol. 2442, pp. 1–16, Springer, 2002.
13. National Bureau of Standards. Data Encryption Standard. FIPS 46. 1977.
14. National Institute of Standards and Technology. Advanced Encryption Standard. FIPS 197. 26 November 2001.
15. National Institute of Standards and Technology. Digital Signature Standard. FIPS 186. 1994.
16. R.L. Rivest, A. Shamir and L.M. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communications of the ACM*, vol. 21, pp. 120-126, 1978.