A Zero-Dimensional Gröbner Basis for AES-128

Johannes Buchmann, Andrei Pyshkin[⋆], Ralf-Philipp Weinmann
{buchmann,pyshkin,weinmann}@cdc.informatik.tu-darmstadt.de

Technische Universität Darmstadt, Fachbereich Informatik,
Hochschulstr. 10, D-64289 Darmstadt, Germany

Abstract. We demonstrate an efficient method for computing a Gröbner basis of a zero-dimensional ideal describing the key-recovery problem from a single plaintext/ciphertext pair for the full AES-128. This Gröbner basis is relative to a degree-lexicographical order. We investigate whether the existence of this Gröbner basis has any security implications for the AES.

Keywords: block ciphers, Gröbner bases, AES, Rijndael

1 Introduction

Gröbner bases are standard representations of polynomial ideals that possess several useful properties:

- given a Gröbner basis of an ideal $I \subset R$, we can efficiently decide whether a polynomial $f \in R$ lies in I
- for suitable term orders (e.g. lexicographical orders), the variety of the ideal can be efficiently computed; this yields solutions for the polynomial system induced by the ideal.

Usually, the Gröbner basis of a set of polynomials is computed using either a variant of Buchberger's algorithm [3] or using Faugere's F_4 [10] or F_5 [11] algorithm. These algorithms involve polynomials reductions which are costly. In general the time and the space complexity of these algorithms is difficult to predict. For polynomials in a large number of variables, these algorithms quickly become infeasible.

Rijndael, the block cipher that has been selected as the Advanced Encryption Standard (AES) in 2001, has become the industry-wide standard block cipher by now. Its design, the wide-trail strategy, is considered state of the art. However, Rijndael has from the beginning been critized for its mathematical simplicity and rich algebraic structure [15, 13, 8]. On the other hand this criticism has not yet substantiated into an attack; quite to the contrary, claims of an algebraic attack using XSL [8] have recently been debunked [6].

[⋆] Supported by a stipend of the Marga und Kurt-Möllgaard-Stiftung.

For the Rijndael block cipher, two algebraic representations in the form of multivariate polynomial systems of equations have been proposed so far. Courtois and Pieprzyk have demonstrated how to obtain overdefined systems of quadratic equations over $GF(2)$, while Murphy and Robshaw have constructed an embedding for the AES called Big Encryption System (BES) for which a system of overdefined quadratic equations over $GF(2^8)$ exists [16].

A representation considering the output of the S-Box as a polynomial expression of the input over $GF(2^8)$ has thus far been neglected because the polynomials in this case are of relatively high degree. Using this representation we can describe the key recovery problem for the AES cipher with a key length of 128 bits as a system of 200 polynomial equations of degree 254 and 152 linear equations. In this paper we will show that by choosing an appropriate term order and by applying linear operations only, we can generate a Gröbner basis for AES-128 from this system without a single polynomial reduction.

The structure of this paper is as follows: in Section 2 we establish the notation used in this paper, in Section 3 we explain how to construct the Gröbner basis for Rijndael, in Section 4 we study the cryptanalytic importance of our result. Finally we summarize the impact of our result in Section 5 and conclude.

2 Notation

We assume the reader to be familiar with the description of AES as given in [17]. In the following we restrict ourselves to AES-128, i.e. Rijndael with a block and key size of 128 bits.

We will deviate from the standard representation by using a column vector instead of a matrix for the internal state and the round keys. The elements in the column vector are identified with the elements of the matrix in a column-wise fashion by the following map:

$$\varphi\colon F^{4\times 4}\to F^{16},\ \begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{pmatrix} \mapsto (s_{0,0}, s_{1,0}, \ldots, s_{0,1}, s_{1,1}, \ldots)^T \qquad (1)$$

Furthermore we define the 16×16 matrix P to be the permutation matrix that achieves the exchange of elements in the column vector that is equivalent to transposing the state matrix.

The above notation allows us to express the diffusion performed by the `MixColumns` and `ShiftRows` operations as a single matrix multiplication.

Let $x_{i,j}$ denote the variable referring to the ith component of the state vector after the jth round execution. By this definition the variables $x_{i,0}$ are called *plaintext variables*, correspondingly $x_{i,10}$ are called *ciphertext variables.* All other variables $x_{i,j}$ are called *intermediate state variables*; variables $k_{i,j}$ are called *key variables.* We will also refer to $k_{i,0}$ as *cipher key variables.*

The field F is the finite field $GF(2^8)$ as defined for Rijndael. The polynomial ring R is defined as

$$R := F[x_{i,j}, k_{i,j} : \{0 \leq i \leq 15, 0 \leq j \leq 10\}]$$

3 Construction of the Gröbner Basis

In this section we will explain how to construct a degree lexicographical Gröbner basis describing the AES key recovery problem step by step. To accomplish this task we will first give a very minimal introduction to Gröbner bases; just enough to follow this paper. We kindly refer the inclined reader to [9] and [2] for a more gentle introduction to the topic.

3.1 Gröbner Bases

Some confusion regularly arises out of the expressions *term* and *monomial.* One school calls a product of variables a *term* and the product of said term and a coefficient a *monomial*; notably this is done in [2]. The other camp, e.g. the authors of [9], uses *term* and *monomial* in an interchanged fashion. We adopt the conventions of [2].

For a given ideal there usually exists more than one Gröbner basis. These are relative to a so called term order, which we shall now define:

Definition 1 (Term order). *A term order $\leq$ is a linear order on the set of terms $\mathcal{T}(R)$ such that*

1. *$1 \leq t$ for all terms $t \in \mathcal{T}(R)$*
2. *for all terms $s, t_1, t_2 \in \mathcal{T}(R)$ whenever $t_1 \leq t_2$ then $st_1 \leq st_2$*

The maximum element of the set of terms of a polynomial p under a fixed term order $\leq$ shall be referred to as the head term of p, short $HT(p)$.

We will now introduce two useful and widely used term orders. First, however, we define two technicalities: For a term $t = \mathfrak{v}_1^{e_1}\mathfrak{v}_2^{e_2} \cdots \mathfrak{v}_k^{e_k} \in \mathcal{T}(R)$ we define the *exponent vector* of t to be $\epsilon(t) = (e_1, e_2, \ldots, e_k) \in \mathbb{N}_0^k$. The total degree of the term t then is $\deg(t) = \sum_{i=1}^{k} e_i$.

Example 1 (lexicographical term order). For terms s, t we define $s <_{lex} t$ iff there exists an i with $1 \leq i \leq k$ such that the first $i-1$ components of $\epsilon(s)$ and $\epsilon(t)$ are equal but the ith component of $\epsilon(s)$ is smaller than the ith component of $\epsilon(t)$.

Example 2 (degree lexicographical term order). For terms s, t we define $s <_{dlex} t$ iff either $\deg(s) < \deg(t)$ or if $\deg(s) = \deg(t)$ and $s <_{lex} t$.

Remark 1. Note that there is more than one lexicographical order and more than one degree lexicographical term order. Different orderings on the variables induce different term orders!

The formal definition of a Gröbner basis does not give much insight about how to construct one:

Definition 2 (Gröbner basis). *Let $\mathcal{I}$ be an ideal of R. A set of polynomials $\{g_1, \ldots, g_m\} \subset \mathcal{I}$ is a Gröbner basis if the following holds:*

$$\langle HT(g_1), \ldots, HT(g_m) \rangle = \langle \{HT(p) : p \in I\} \rangle$$

The first Buchberger criterion [4] is a basic test that is used in most implementations of Buchberger's algorithm to avoid "useless" polynomial reductions. The following theorem follows almost instantaneously from this criterion and gives an important hint how a Gröbner basis can be attained without knowing anything about polynomial reductions.

Theorem 1. *Let G be a set of polynomials and $H = \{HT(f) : f \in G\}$. If all elements in H are pairwise prime, then G is a Gröbner basis.*

Proof. See [5].

A zero-dimensional ideal is an ideal that has a finite number of solutions over the closure of the field. It usually is advantageous to have this property for Gröbner basis computations. By using Corollary 6.56 of [2] we can determine whether an ideal I is zero-dimensional. Below we state a reduced version of this corollary:

Lemma 1. *Let I be a proper ideal of $F[x_1, \ldots, x_n]$. Then the following assertions are equivalent:*

- $\dim(I) = 0$
- *There exists a term order $\leq$ such that for each $1 \leq i \leq n$ there is $g_i \in I$ with $HT(g_i) = x_i^{\nu_i}$ for some $0 \leq \nu_i \in \mathbb{N}$.*

3.2 The S-Box

The S-Box used in Rijndael can be interpolated as a sparse polynomial over F:

$$\sigma : F \to F, \quad x \mapsto \texttt{05}x^{254} + \texttt{09}x^{253} + \texttt{F9}x^{251} + \texttt{25}x^{247} + \texttt{F4}x^{239} + \\ \texttt{B5}x^{223} + \texttt{B9}x^{191} + \texttt{8F}x^{127} + \texttt{63} \tag{2}$$

whilst the interpolation polynomial of the inverse S-Box

$$\sigma^{-1} : F \to F, \quad x \mapsto \sum_{i=0}^{254} c_i x^i \tag{3}$$

is dense. This polynomial is given in Appendix A.

3.3 The Linear Transformation

The linear transformation of AES consists of two operations, `ShiftRows` and `MixColumns`. We can perform the linear transform by multiplying the state column vector with a 16 × 16-matrix D from the left. In the following, we calculate D; however at the start of each round we apply the transposition matrix P since it makes expressing the operations as matrices easier. At the end we multiply with the matrix P to undo the initial transposition.

A matrix that shifts the elements of a 1 × 4 row vector cyclically by an offset t is of the following form:

$$D_{\mathrm{SR_t}} = \left(\Delta_{i,(j-t) \bmod 4}\right) \in F^{4\times 4} \tag{4}$$

where $\Delta_{i,j}$ is the Kronecker delta. The `ShiftRows` operation is equivalent to multiplying by the matrix D_{SR}:

$$D_{\mathrm{SR}} = \begin{pmatrix} D_{\mathrm{SR_0}} & 0 & 0 & 0 \\ 0 & D_{\mathrm{SR_1}} & 0 & 0 \\ 0 & 0 & D_{\mathrm{SR_2}} & 0 \\ 0 & 0 & 0 & D_{\mathrm{SR_3}} \end{pmatrix} \in F^{16\times 16} \tag{5}$$

The `MixColumns` operation is applied to each row of the internal state. We use the matrix D_{MC} to transform the column vector equivalently:

$$D_{\mathrm{MC}} = \begin{pmatrix} \texttt{02 03 01 01} \\ \texttt{01 02 03 01} \\ \texttt{01 01 02 03} \\ \texttt{03 01 01 02} \end{pmatrix} \otimes I_4 \in F^{16\times 16} \tag{6}$$

where $\otimes$ denotes the tensor product. Concatenation of the two operations in the diffusion layer is achieved by multiplying the above matrices, yielding the matrix D:

$$D = P \cdot D_{\mathrm{MC}} \cdot D_{\mathrm{SR}} \cdot P \tag{7}$$

The diffusion layer of the last round is missing the `MixColumns` transformation; it will be described by the matrix $\tilde{D}$:

$$\tilde{D} = P \cdot D_{\mathrm{SR}} \cdot P \tag{8}$$

This enables us to obtain the following vectorial representation of a system of 16 polynomial equations that holds for rounds $1 \leq j \leq 9$ of the cipher:

$$\begin{pmatrix} \sigma(x_{0,(j-1)} + k_{0,(j-1)}) \\ \vdots \\ \sigma(x_{15,(j-1)} + k_{15,(j-1)}) \end{pmatrix} + D^{-1} \begin{pmatrix} x_{0,j} \\ \vdots \\ x_{15,j} \end{pmatrix} = 0 \tag{9}$$

For the last round we need to take the simplified diffusion layer and the final key addition into account:

$$\begin{pmatrix} \sigma\left(x_{0,9} + k_{0,9}\right) \\ \vdots \\ \sigma\left(x_{15,9} + k_{15,9}\right) \end{pmatrix} + \tilde{D}^{-1} \begin{pmatrix} x_{0,10} + k_{0,10} \\ \vdots \\ x_{15,10} + k_{15,10} \end{pmatrix} = 0 \tag{10}$$

Choosing any degree lexicographical term order, either a term $x_{i,j}^{254}$ or a term $k_{i,j}^{254}$ occurs as head term of each polynomial. We take note that none of the head terms is a power of a plaintext nor of a ciphertext variable. Moreover all of the head terms are pairwise prime. The variable order chosen will influence whether the head term is a power of a key variable or of an intermediate state variable.

3.4 The Key Schedule

In order to obtain a Gröbner basis of both the cipher and the key scheduling polynomials, we need to set up the key scheduling in a slightly different way. Usually, the key scheduling expresses the elements of the round subkey of round $1 \leq j \leq 10$ as a vector of polynomials in the key variables of the previous round as follows:

$$\begin{pmatrix} k_{0,j} \\ k_{1,j} \\ k_{2,j} \\ k_{3,j} \\ k_{4,j} \\ \vdots \\ k_{15,j} \end{pmatrix} = \begin{pmatrix} k_{0,j-1} \\ k_{1,j-1} \\ k_{2,j-1} \\ k_{3,j-1} \\ k_{4,j-1} \\ \vdots \\ k_{15,j-1} \end{pmatrix} + \begin{pmatrix} \sigma(k_{15,j-1}) \\ \sigma(k_{12,j-1}) \\ \sigma(k_{13,j-1}) \\ \sigma(k_{14,j-1}) \\ k_{0,j} \\ \vdots \\ k_{11,j} \end{pmatrix} + \begin{pmatrix} \gamma_{j-1} \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{11}$$

where the $\gamma_0, \ldots, \gamma_9$ are the round constants. To make all head terms pairwise prime (see also Section 3.5 on the term order chosen), we we have to proceed in reverse order:

$$\begin{pmatrix} \sigma^{-1}(k_{0,j} + k_{0,j-1} + \gamma_{j-1}) \\ \sigma^{-1}(k_{1,j} + k_{1,j-1}) \\ \sigma^{-1}(k_{2,j} + k_{2,j-1}) \\ \sigma^{-1}(k_{3,j} + k_{3,j-1}) \\ k_{4,j} + k_{4,j-1} \\ \vdots \\ k_{15,j} + k_{15,j-1} \end{pmatrix} + \begin{pmatrix} k_{15,j-1} \\ k_{12,j-1} \\ k_{13,j-1} \\ k_{14,j-1} \\ k_{0,j} \\ \vdots \\ k_{11,j} \end{pmatrix} = 0 \tag{12}$$

3.5 Choosing a Suitable Variable Order

The plaintext and ciphertext polynomials simply are of the form

$$x_{i,0} + p_i \qquad p_i \in F, 0 \leq i \leq 15 \tag{13}$$

respectively

$$x_{i,0} + c_i \qquad c_i \in F, 0 \leq i \leq 15. \tag{14}$$

Let $\mathcal{A}$ be the union of the left-hand side of equations (9), (10) and (12) for all rounds $1 \leq j \leq 10$ as well as the plaintext and ciphertext polynomials. Ordering the variables as follows makes all head terms pairwise prime:

1. plaintext variables: $x_{0,0} < \ldots < x_{15,0}$
2. ciphertext variables: $x_{0,10} < \ldots < x_{15,10}$
3. key variables of all rounds in natural order: $k_{0,0} < k_{1,0} < \ldots < k_{15,10}$
4. intermediate state variables in their natural order

The degree lexicographical term order with the above variable order will be in the following be referred to as $<_{\mathcal{A}}$. By Theorem 1, the set of polynomials $\mathcal{A}$ is a Gröbner basis relative to this term order! Moreover, checking Lemma 1 we verify that this ideal is zero-dimensional.

4 Exploiting the Gröbner Basis

In the previous section we have shown how to obtain a zero-dimensional Gröbner basis $\mathcal{A}$ for AES-128. In this section we explore the cryptanalytic impact of this finding. To this end, we investigate the complexity of a Gröbner basis conversion algorithm, find an invariant under the elimination of variables and explain why the naïve way of applying the ideal membership test does not work for guessing parts of the round key.

4.1 Complexity of Gröbner Basis Conversions

An obvious question is whether the Gröbner basis we have computed in the previous section can be efficiently converted to a different, more suitable order, i.e. a lexicographical order or an elimination order [1].

Two algorithms and variations of them are known for performing Gröbner basis conversions, the FGLM algorithm [12] and the Gröbner Walk [7]. While the FGLM algorithm as described in [12] only works for zero-dimensional ideals, the Gröbner Walk naturally also works for ideals of positive dimension. Since we have established that $\mathcal{A}$ is zero-dimensional, we are in a position to use FGLM and give an estimate for its time complexity below.

An important characteristic of the ideal is the vector space dimension of the residue class ring obtained when factoring the polynomial ring R by the ideal I:

Definition 3. *Let $R := F[x_1, \ldots, x_n]$. Then the F-space dimension of the ideal $I \subset R$ shall be denoted by* $\dim(R/I)$.

From Lemma 6.51 and Proposition 6.52 in [2] it is straightforward to deduce the following lemma:

Lemma 2. *Let $\leq$ be a term order on $\mathcal{T}(R)$ and G a Gröbner basis of I w.r.t. $\leq$. Then*

$$\begin{aligned}\dim(R/I) &= \#\left\{t \in \mathcal{T}(R) : s \nmid t \textit{ for all } s \in HT(I)\right\}\\ &= \#\left\{t \in \mathcal{T}(R) : s \nmid t \textit{ for all } s \in HT(G)\right\}\end{aligned}$$

Applying the lemma to a Gröbner basis with univariate head terms yields the following corollary:

Corollary 1. *Let $G = \{g_1, \ldots, g_n\}$ be a Gröbner basis for the ideal $I \subset F[x_1, \ldots, x_n]$ with head terms $x_1^{d_1}, \ldots, x_n^{d_n}$. Then* $\dim(R/I) = d_1 \cdot \cdots \cdot d_n$.

This result is sufficient to give a bound on the complexity of the Gröbner basis conversion using FGLM. The following theorem is a slightly rephrased version of Theorem 5.1 in [12]:

Theorem 2. *Let F be a finite field and $R = F[x_1, \ldots, x_n]$. Furthermore $G_1 \subset R$ is the Gröbner basis relative to a term order $<_1$ of an ideal I, and $D = dim(R/I)$. We can then convert G_1 into a Gröbner basis G_2 relative to a term order $<_2$ in $O(nD^3)$ field operations.*

From Corollary 1 we conclude that the vector space dimension of the ideal generated by the Gröbner basis $\mathcal{A}$ is way too big for the FGLM algorithm be useful for cryptanalytic purposes in this case:

$$dim(R/\mathcal{A}) = 254^{200} \approx 2^{1598} \tag{15}$$

For the Gröbner Walk, the running time strongly depends on the source and the target term order. It is an open problem to give bounds on the time and space complexity for this algorithm. The only bounds known are local bounds, namely for adjacent term orders, due to Kalkbrener [14].

4.2 Elimination of Variables

In this section we establish that the dimension of the vector space of the ideal remains invariant when eliminating certain variables. We first prove the following more general statement:

Proposition 1. *Let I' be a zero-dimensional ideal of $R' := F[x_1, \ldots, x_n]$, I an ideal of $R := R'[x_{n+1}]$ and $I' = I \cap R'$. Then $\dim R/I = \dim R'/I'$ iff there exists a polynomial $g \in R'$ such that $x_{n+1} + g \in I$.*

Proof. W.l.o.g. we fix a lexicographical term ordering such that x_{n+1} is the greatest variable. Let $\mathrm{RT}(I)$ and $\mathrm{RT}(I')$ be defined as follows:

$$\begin{aligned} \mathrm{RT}(I) &= \{t \in \mathcal{T}(R) : s \nmid t \text{ for all } s \in \mathrm{HT}(I)\} \\ \mathrm{RT}(I') &= \left\{t \in \mathcal{T}(R') : s \nmid t \text{ for all } s \in \mathrm{HT}(I')\right\} \subset \mathrm{RT}(I) \end{aligned}$$

By Lemma 2, $\dim_K(R/I) = \#\mathrm{RT}(I)$ holds. Thus it is sufficient to prove that $\#\mathrm{RT}(I) = \#\mathrm{RT}(I')$. Since $x_{n+1} \nmid t$ for $t \in \mathcal{T}(R')$, the equality $\mathrm{RT}(I) = \mathrm{RT}(I')$ holds iff $x_{n+1} \in \mathrm{HT}(I)$, i.e. exists a $g \in R'$ for which $x_{n+1} + g \in I$.
□

Corollary 2. *For the set of polynomials $\mathcal{A}$ the dimension* $\dim(R/I)$ *is invariant under the elimination of all variables except the round key variables* $k_{i,0}$ *with* $0 \leq i \leq 15$ *and* $k_{i,j}$ *with* $0 \leq i \leq 3,\ 1 \leq j \leq 9$.

Proof. By induction using Proposition 1.

So even eliminating a significant amount of variables does not reduce the complexity of converting the Gröbner basis to a term order suitable for key recovery.

4.3 Taking the Field Equations into Account

Let $R = F[x_1, \ldots, x_n]$ be a polynomial ring over finite field $F = GF(2^m)$ with $q = 2^m$ elements. For every element $\tau \in F$ the relation $\tau^q = \tau$ holds; the equations

$$x_i^q + x_i = 0 \tag{16}$$

are commonly called *field equations*. The set of roots of each of these equations is the set of all elements of the field F. By adjoining the set of all field polynomials $\mathcal{F}$ — the left-hand side of Equation 16 — to the set of polynomials $\mathcal{A}$, we eliminate all points of the variety that only exist in the closure but not in the ground field. The resulting set does not form a Gröbner basis, however.

What we have to do is to compute the intersection of two varieties; this is usually achieved by computing the Gröbner basis of the sum of the corresponding ideals. We have a set of polynomials $\mathcal{A}$, describing AES which is a Gröbner basis relative to the order $<_{\mathcal{A}}$, and a second set of polynomials $\mathcal{F}$, which also forms a Gröbner basis relative to the same order. It is however unclear how to exploit the Gröbner basis property of the input.

4.4 Testing Keys

Gröbner bases were invented to solve the ideal membership problem. So why are we not able to simply test whether a linear polynomial of the form

$$k_i + C, \qquad C \in F \tag{17}$$

— with C being a key variable guess — lies in the ideal? After all, this would allow us to determine the key piecementally by guessing each byte.

Several problems present themselves here. First of all, the polynomial system has solutions over the closure of the ground field, which means that we have to test for a polynomial

$$g = p \cdot \prod (k_i + C_j)^{t_j}, \quad t_j \in \mathbb{N}_0,\ C_j \in F$$

instead, where the C_j denote candidate values for the key variable and p is a product of irreducible non-linear polynomials. Moreover the dimension of the ideal again plays an important role here: it is an upper bound on the number of solutions of the corresponding polynomial system in the closure of the field. Hence the degree of g is expected to be very large.

5 Implications

As far as the authors are aware at the time of writing this paper, the existence of the above Gröbner basis has no security implications for AES. We conjecture that methods similar to the one presented in this paper can be used to produce total-degree Gröbner bases for many other iterated block ciphers – however we like to point out that because of the high algebraic structure of Rijndael, it makes for an excellent example.

6 Conclusion

We have demonstrated that by choosing a particular variable order, degree lexicographical Gröbner bases for AES-128 can be constructed without polynomial reductions. We have analyzed the implications of this finding and have shown that several obvious approaches do not translate into a successful cryptanalysis. It is an open problem whether the results contained in this paper can be leveraged into an attack.

7 Acknowledgments

The third author acknowledges several insightful discussions with Frederik Armknecht.

References

1. David Bayer and Michael Stillman. On the complexity of computing syzygies. *Journal of Symbolic Computation*, 6(2/3):135–147, 1988.

2. Thomas Becker and Volker Weispfenning. *Gröbner Bases – A Computational Approach to Commutative Algebra*. Springer-Verlag, 1991.
3. Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, University of Innsbruck, Austria, 1965.
4. Bruno Buchberger. A criterion for Detecting Unnecessary Reductions in the Construction of Groebner Bases. volume 72, pages 3–21, London, UK, 1979. Johannes Kepler University Linz, Springer, Berlin - Heidelberg - New York.
5. Johannes Buchmann, Andrei Pyshkin, and Ralf-Philipp Weinmann. Block Ciphers Sensitive to Gröbner Basis Attacks. In *Topics in Cryptology - CT-RSA 2006*, volume 3860 of *Lecture Notes in Computer Science*, pages 313–331. Springer, 2006.
6. Carlos Cid and Gaëtan Leurent. An analysis of the XSL Algorithm. In Roy Bimal, editor, *Advances in Cryptology – ASIACRYPT 2005*, volume 3788 of *Lecture Notes in Computer Science*, pages 333–345. Springer, 2005.
7. Stéphane Collart, Michael Kalkbrener, and Daniel Mall. Converting Bases with the Gröbner Walk. *Journal of Symbolic Computation*, 24(3/4):465–469, 1997.
8. Nicolas Courtois and Josef Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. In Yuliang Zheng, editor, *Advances in Cryptology – ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 267–287. Springer, 2002.
9. David A. Cox, John B. Little, and Don O'Shea. *Ideals, Varieties, and Algorithms.* Springer-Verlag, NY, 2nd edition, 1996. 536 pages.
10. Jean-Charles Faugère. A New Efficient Algorithm for Computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1-3):61–88, June 1999.
11. Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *Symbolic and Algebraic Computation – ISSAC 2002*, pages 75–83. ACM, 2002.
12. Jean-Charles Faugère, P. Gianni, Daniel Lazard, and Teo Mora. Efficient Computation of Zero-Dimensional Gröbner Bases by Change of Ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.
13. Niels Ferguson, Richard Schroeppel, and Doug Whiting. A Simple Algebraic Representation of Rijndael. In Serge Vaudenay and Amr M. Youssef, editors, *Selected Areas in Cryptography*, volume 2259 of *Lecture Notes in Computer Science*, pages 103–111. Springer, 2001.
14. Michael Kalkbrener. On the Complexity of Gröbner Bases Conversion. *Journal of Symbolic Computation*, 28(1-2):265–273, 1999.
15. Sean Murphy and Matt Robshaw. Further Comments on the Structure of Rijndael. AES Comment to NIST, August 2000.
16. Sean Murphy and Matthew J.B. Robshaw. Essential Algebraic Structure within the AES. In Moti Yung, editor, *Advances in Cryptology – CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 1–16. Springer, 2002.
17. National Institute of Standards and Technology. FIPS-197: Advanced Encryption Standard, November 2001. Available at http://csrc.nist.gov/publications/fips/.

A Polynomial interpolation of the inverse S-Box of Rijndael

$$\begin{aligned}
&\sigma^{-1} : F \longrightarrow F\\
x \mapsto\ &\mathtt{05}x^{254}+\mathtt{CF}x^{253}+\mathtt{B3}x^{252}+\mathtt{16}x^{251}+\mathtt{55}x^{250}+\mathtt{C0}x^{249}+\mathtt{7A}x^{248}+\mathtt{01}x^{247}+\\
&\mathtt{22}x^{246}+\mathtt{D8}x^{245}+\mathtt{6B}x^{244}+\mathtt{A6}x^{243}+\mathtt{1F}x^{242}+\mathtt{0D}x^{241}+\mathtt{BC}x^{240}+\mathtt{49}x^{239}+\\
&\mathtt{85}x^{238}+\mathtt{B4}x^{237}+\mathtt{1B}x^{236}+\mathtt{5E}x^{235}+\mathtt{BD}x^{234}+\mathtt{18}x^{233}+\mathtt{1D}x^{232}+\mathtt{6D}x^{231}+\\
&\mathtt{C5}x^{230}+\mathtt{23}x^{229}+\mathtt{09}x^{228}+\mathtt{43}x^{227}+\mathtt{68}x^{226}+\mathtt{80}x^{225}+\mathtt{6C}x^{224}+\mathtt{CC}x^{223}+\\
&\mathtt{42}x^{222}+\mathtt{9F}x^{221}+\mathtt{0F}x^{220}+\mathtt{D2}x^{219}+\mathtt{3B}x^{218}+\mathtt{2C}x^{217}+\mathtt{5F}x^{216}+\mathtt{BE}x^{215}+\\
&\mathtt{AE}x^{214}+\mathtt{E4}x^{213}+\mathtt{93}x^{212}+\mathtt{8B}x^{211}+\mathtt{CB}x^{210}+\mathtt{65}x^{209}+\mathtt{C0}x^{208}+\mathtt{1E}x^{207}+\\
&\mathtt{8E}x^{206}+\mathtt{32}x^{205}+\mathtt{1D}x^{204}+\mathtt{A5}x^{203}+\mathtt{76}x^{202}+\mathtt{A9}x^{201}+\mathtt{2C}x^{200}+\mathtt{13}x^{199}+\\
&\mathtt{05}x^{198}+\mathtt{60}x^{197}+\mathtt{FD}x^{196}+\mathtt{1B}x^{195}+\mathtt{AB}x^{194}+\mathtt{64}x^{193}+\mathtt{C1}x^{192}+\mathtt{A8}x^{191}+\\
&\mathtt{7F}x^{190}+\mathtt{55}x^{189}+\mathtt{DB}x^{188}+\mathtt{EC}x^{187}+\mathtt{20}x^{186}+\mathtt{C4}x^{185}+\mathtt{DB}x^{184}+\mathtt{7E}x^{183}+\\
&\mathtt{92}x^{182}+\mathtt{80}x^{181}+\mathtt{A3}x^{180}+\mathtt{59}x^{179}+\mathtt{91}x^{178}+\mathtt{91}x^{177}+\mathtt{81}x^{176}+\mathtt{4E}x^{175}+\\
&\mathtt{11}x^{174}+\mathtt{DD}x^{173}+\mathtt{4E}x^{172}+\mathtt{D3}x^{171}+\mathtt{E3}x^{170}+\mathtt{19}x^{169}+\mathtt{E7}x^{168}+\mathtt{03}x^{167}+\\
&\mathtt{24}x^{166}+\mathtt{45}x^{165}+\mathtt{DA}x^{164}+\mathtt{EA}x^{163}+\mathtt{87}x^{162}+\mathtt{2D}x^{161}+\mathtt{23}x^{160}+\mathtt{82}x^{159}+\\
&\mathtt{38}x^{158}+\mathtt{B7}x^{157}+\mathtt{9E}x^{156}+\mathtt{B3}x^{155}+\mathtt{2A}x^{154}+\mathtt{3E}x^{153}+\mathtt{1C}x^{152}+\mathtt{EC}x^{151}+\\
&\mathtt{C3}x^{150}+\mathtt{45}x^{149}+\mathtt{ED}x^{148}+\mathtt{D5}x^{147}+\mathtt{2A}x^{146}+\mathtt{8D}x^{145}+\mathtt{ED}x^{144}+\mathtt{37}x^{143}+\\
&\mathtt{26}x^{142}+\mathtt{E0}x^{141}+\mathtt{BC}x^{140}+\mathtt{58}x^{139}+\mathtt{E2}x^{138}+\mathtt{6C}x^{137}+\mathtt{24}x^{136}+\mathtt{55}x^{135}+\\
&\mathtt{C7}x^{134}+\mathtt{AA}x^{133}+\mathtt{09}x^{132}+\mathtt{4F}x^{131}+\mathtt{82}x^{130}+\mathtt{CA}x^{129}+\mathtt{10}x^{128}+\mathtt{EE}x^{127}+\\
&\mathtt{1A}x^{126}+\mathtt{2E}x^{125}+\mathtt{40}x^{124}+\mathtt{27}x^{123}+\mathtt{81}x^{122}+\mathtt{92}x^{121}+\mathtt{B1}x^{120}+\mathtt{02}x^{119}+\\
&\mathtt{8B}x^{118}+\mathtt{87}x^{117}+\mathtt{7F}x^{116}+\mathtt{B0}x^{115}+\mathtt{6F}x^{114}+\mathtt{53}x^{113}+\mathtt{08}x^{112}+\mathtt{CB}x^{111}+\\
&\mathtt{03}x^{110}+\mathtt{B0}x^{109}+\mathtt{DF}x^{108}+\mathtt{1F}x^{107}+\mathtt{A7}x^{106}+\mathtt{A2}x^{105}+\mathtt{FE}x^{104}+\mathtt{8E}x^{103}+\\
&\mathtt{A8}x^{102}+\mathtt{E1}x^{101}+\mathtt{71}x^{100}+\mathtt{FF}x^{99}+\mathtt{55}x^{98}+\mathtt{5A}x^{97}+\mathtt{1D}x^{96}+\mathtt{9D}x^{95}+\\
&\mathtt{BF}x^{94}+\mathtt{E8}x^{93}+\mathtt{BA}x^{92}+\mathtt{6B}x^{91}+\mathtt{72}x^{90}+\mathtt{E3}x^{89}+\mathtt{04}x^{88}+\mathtt{D9}x^{87}+\\
&\mathtt{38}x^{86}+\mathtt{D3}x^{85}+\mathtt{B9}x^{84}+\mathtt{16}x^{83}+\mathtt{52}x^{82}+\mathtt{18}x^{81}+\mathtt{19}x^{80}+\mathtt{3E}x^{79}+\\
&\mathtt{9E}x^{78}+\mathtt{03}x^{77}+\mathtt{56}x^{76}+\mathtt{A6}x^{75}+\mathtt{71}x^{74}+\mathtt{03}x^{73}+\mathtt{E4}x^{72}+\mathtt{86}x^{71}+\\
&\mathtt{F5}x^{70}+\mathtt{B0}x^{69}+\mathtt{05}x^{68}+\mathtt{D1}x^{67}+\mathtt{10}x^{66}+\mathtt{E2}x^{65}+\mathtt{E5}x^{64}+\mathtt{CB}x^{63}+\\
&\mathtt{B1}x^{62}+\mathtt{F2}x^{61}+\mathtt{8E}x^{60}+\mathtt{C7}x^{59}+\mathtt{0C}x^{58}+\mathtt{A7}x^{57}+\mathtt{BF}x^{56}+\mathtt{46}x^{55}+\\
&\mathtt{0B}x^{54}+\mathtt{01}x^{53}+\mathtt{C5}x^{52}+\mathtt{A3}x^{51}+\mathtt{50}x^{50}+\mathtt{77}x^{49}+\mathtt{EA}x^{48}+\mathtt{05}x^{47}+\\
&\mathtt{65}x^{46}+\mathtt{8E}x^{45}+\mathtt{89}x^{44}+\mathtt{D4}x^{43}+\mathtt{6D}x^{42}+\mathtt{D3}x^{41}+\mathtt{75}x^{40}+\mathtt{65}x^{39}+\\
&\mathtt{13}x^{38}+\mathtt{2F}x^{37}+\mathtt{86}x^{36}+\mathtt{AF}x^{35}+\mathtt{7C}x^{34}+\mathtt{7B}x^{33}+\mathtt{85}x^{32}+\mathtt{C8}x^{31}+\\
&\mathtt{E8}x^{30}+\mathtt{04}x^{29}+\mathtt{7B}x^{28}+\mathtt{CF}x^{27}+\mathtt{2F}x^{26}+\mathtt{8A}x^{25}+\mathtt{9A}x^{24}+\mathtt{3D}x^{23}+\\
&\mathtt{CF}x^{22}+\mathtt{21}x^{21}+\mathtt{39}x^{20}+\mathtt{D9}x^{19}+\mathtt{29}x^{18}+\mathtt{73}x^{17}+\mathtt{F6}x^{16}+\mathtt{23}x^{15}+\\
&\mathtt{40}x^{14}+\mathtt{1B}x^{13}+\mathtt{B2}x^{12}+\mathtt{C0}x^{11}+\mathtt{6D}x^{10}+\mathtt{85}x^{9}+\mathtt{1C}x^{8}+\mathtt{8A}x^{7}+\\
&\mathtt{2C}x^{6}+\mathtt{BB}x^{5}+\mathtt{90}x^{4}+\mathtt{1E}x^{3}+\mathtt{7E}x^{2}+\mathtt{F3}x^{1}+\mathtt{52}
\end{aligned}$$