Cryptanalysis of Block Ciphers with Probabilistic Non-linear Relations of Low Degree

Thomas Jakobsen

Department of Mathematics, Building 303, Technical University of Denmark, DK-2800 Lyngby, Denmark, email: T.Jakobsen@mat.dtu.dk

Abstract. Using recent results from coding theory, it is shown how to break block ciphers operating on GF(q) where the ciphertext is expressible as evaluations of an unknown univariate polynomial of low degree m over the plaintext with a typically low but non-negligible probability μ. The method employed is essentially Sudan's algorithm for decoding Reed-Solomon codes beyond the error-correction diameter. The known-plaintext attack needs $n = 2m/\mu^2$ plaintext/ciphertext pairs and the running time is polynomial in n. Furthermore, it is shown how to discover more general non-linear relations $p(x, y) = 0$ between plaintext x and ciphertext y that hold with small probability μ. The second attack needs access to $n = (2m/\mu)^2$ plaintext/ciphertext pairs where $m = \deg p$ and its running time is also polynomial in n. As a demonstration, we break up to 10 rounds of a cipher constructed by Nyberg and Knudsen provably secure against differential and linear cryptanalysis.
Key words: Cryptanalysis, block cipher, interpolation attack, non-linear relations, Reed-Solomon codes, Sudan's algorithm.

1 Introduction

For some block ciphers, the round function can be described by a low degree polynomial for a non-negligible fraction of its input values. This may happen if there are bad S-boxes or if simple algebraic functions are used unwisely. (Some simple functions provide very good immunity against differential and linear cryptanalysis.) This paper shows how one may break such ciphers.

Previous work has focused on either the linear case or the case where the output is always expressible as a low degree polynomial (not just a fraction of the time). For instance, Matsui's linear cryptanalysis [14] is applicable when some of the output bits can be described as a linear combination of the input bits for a sufficient fraction of the possible plaintexts. Jakobsen and Knudsen's interpolation attack [9] demonstrates how to break ciphers for which the ciphertext is always (with probability 1) expressible as a low degree polynomial of the plaintext. Their attack fails when "noise" is introduced. Similarly, Lai's higher order differentials [10] [9] work only in the case where the output is always expressible as a low-degree polynomial of the input.

Assume that the output of some block cipher can be expressed as evaluations of a degree m polynomial for a fraction of μ of its possible inputs. We will say that such a cipher is (m, μ)-expressible. Intuitively, such ciphers appear to be weak. However, the problem of successfully cryptanalyzing (m, μ)-expressible ciphers can be shown to be essentially equivalent to the problem of decoding very low-rate Reed-Solomon codes subject to severe noise (with error rate above $\frac{1}{2}$). Efficient decoding of such codes was not possible until recently where Sudan [17] [18] published a very novel algorithm which is able to correct several more errors in polynomial time.

The paper is organized as follows. First we give some preliminaries in Section 2 and show how to obtain the round keys of a block cipher one at a time given that there exists a method to distinguish random pairs from actual plaintext/ciphertext pairs.

In Section 3, the Reed-Solomon codes and Sudan's result will be explained and in Section 4 an attack using Sudan's algorithm is presented. If there exist low degree polynomials describing the ciphertext for a sufficient number of the inputs, then the algorithm will find them. This information leak gives probabilistic knowledge of the ciphertext. As mentioned above this information in turn can be used to obtain the round keys. As a demonstration we cryptanalyze several rounds of a cipher constructed by Nyberg and Knudsen [15] which is immune to both differential and linear cryptanalysis. We break several rounds faster than exhaustive key search and using less than 2^{32} plaintext/ciphertext pairs (*p/c-pairs*).

Section 5 describes a more general attack. Here the probabilistic relation between plaintext x and ciphertext y has the more general form $p(x, y) = 0$ for some bivariate polynomial p with low degree. We conclude in Section 6 with some comments and by stating possible applications and extensions of the attack.

2 Preliminaries

We consider r-round iterated block ciphers with round function

$$C_i = F_{K_i}(C_{i-1})$$

where C_0 is the plaintext, K is the ith round key, and C_r is the ciphertext. We will assume that F is a bijection taking values in $\mathrm{GF}(q)$, where q is an integer such that a finite field of size q exists. In addition, we assume that the round keys are independent, uniformly distributed, and, moreover, that they are introduced by some group operation in such a way that the cipher is a Markov cipher [12]. Considering plaintext and keys to be random variables this implies that the inputs to each round may be considered independent.

Definition 1. *Given a function* $f : \mathrm{GF}(q) \to \mathrm{GF}(q)$ *and a polynomial* $p : \mathrm{GF}(q) \to \mathrm{GF}(q)$ *we say that* f *is* (m, μ)-expressible *if*

$$f(x) = p(x) \text{ holds with probability at least } \mu, \tag{1}$$

where $\deg(p) \leq m$.

Example 2. Let $a, b \in \mathrm{GF}(2^w)$ and let the function $\mathrm{XOR}(a,b) = a+b$ be defined by the bitwise addition of its arguments. Similarly, let $\mathrm{ADD}(a,b)$ be defined by the modulo-n addition of the arguments considered as elements of $\mathbb{Z}_n$ where $n = 2^w$. These functions are used in several block ciphers to represent "incompatible" groups, e.g. in [11] or [16].

Given two values a and b, if there is no bit position other than the most significant bit where both have a 1, then $\mathrm{XOR}(a,b) = \mathrm{ADD}(a,b)$. In other words, ADD is $\left(1, \left(\frac{3}{4}\right)^{w-1}\right)$-expressible over $\mathrm{GF}(2^w)$.

We now show what happens if one iterates (m,μ)-expressible round functions.

Proposition 3. *Consider an r-round Markov cipher with round function F. Assume that F is (m,μ)-expressible. Then the cipher is (m^r, μ^r)-expressible.*

Note that there may be a better approximation for the whole r-round cipher. However, it is at least (m^r, μ^r)-expressible.

Proof. Consider two applications of F_{k_i}: $y = F_{k_1}(x)$ and $z = F_{k_2}(y)$, i.e., $z = F_{k_2}(F_{k_1}(x))$. Then y is expressible as a polynomial $q_1(x)$ with $\deg(p_1) \leq m$ for a fraction $\mu_1 = \mu$ of the possible values of x. Similarly z is expressible as a polynomial $p_2(y)$ with $\deg(p_2) \leq m$ for a fraction $\mu_2 = \mu$ of the possible values of y.

Since the cipher is a Markov cipher, we may assume that the inputs to each round are statistically independent, and hence z is expressible as a polynomial $p(x) = p_2(p_1(x))$ with $\deg(p) \leq m^2$ for a fraction $\mu_1\mu_2 = \mu^2$ of the possible input values, i.e., it is (m^2, μ^2)-expressible.

The proof is finished by induction on the number of rounds.

If we have a probabilistic relation between plaintext and ciphertext expressed as a polynomial, then we already have an information leakage and the cipher may be considered broken. Indeed, the following proposition shows us how we may divide and conquer using this information to obtain the round keys one at a time, in effect peeling off one round after another. But first we need some definitions.

Definition 4. *Let there be given a set $S = \{(x_i, y_i)\}_{i=1,\ldots,n}$ of pairs and a block cipher. An algorithm which can successfully distinguish a set of p/c-pairs from a set of random pairs is called a* discriminator *(with respect to that cipher).*

Matsui's linear relations, the differential characteristics of Biham and Shamir, and the polynomial relations described above are all examples of useful expressions for discriminators.

The following is a variant of what Harpes, Kramer, and Massey [6] refer to as the hypothesis of wrong-key randomization.

Definition 5. *Let there be given an r-round block cipher C. Define by the* reduced *cipher $\tilde{C}$ the first $r-1$ rounds of C. Additionally, let there be given a set $S = \{(x_i, y_i)\}_{i=1,\ldots,n}$ of p/c-pairs and a discriminator for the reduced cipher $\tilde{C}$.*

Let S_k be the set constructed from S by decrypting the ciphertexts y by one round using last-round key k. Furthermore, let k_c denote the actual (correct) last-round key and let $k_w \neq k_c$ be a wrong guess. The discriminator is said to be compliant *if it successfully distinguishes S_{k_c} from S_{k_w}.*

Informally speaking, the term "wrong-key randomization" comes from the fact that (hopefully) decryption using the wrong last-round key will randomize the p/c-pairs.

Proposition 6. *Given some block cipher C, assume that there exists a compliant discriminator for the corresponding reduced cipher $\tilde{C}$ requiring access to n pairs and running in t steps. Then it is possible to obtain the last round key of C using n p/c-pairs and expected time $\frac{1}{2}t|\mathcal{K}|$ where $\mathcal{K}$ is the key space of the last round.*

Proof. To find the last round key simply make a guess and decrypt the ciphertexts by one round. Then use the discriminator to check if the decryptions belong to the reduced cipher. If this is the case we found the correct key. Otherwise proceed with another guess. There are $|\mathcal{K}|$ possible round keys and the discriminator runs in t steps for an expected running time of $\frac{1}{2}t|\mathcal{K}|$.

Note that an attack like the above might be entirely impractical due to large $|\mathcal{K}|$. The motivation to include Prop. 6, however, was to demonstrate how an information leak can sometimes be exploited to break a cipher entirely. The existence of a polynomial approximation in itself is usually enough to consider a cipher broken.

3 Reed-Solomon Codes

The Reed-Solomon codes [13] are a class of linear codes over the alphabet GF(q). The $[n, k]_q$ Reed-Solomon code, where n is the length (usually $n = q - 1$) and k is the dimension of the code is obtained by letting each message $r = r_0 \dots r_{k-1}$ denote the coefficients of a degree $k - 1$ polynomial $p(x) = \sum_{i=0}^{k-1} r_i x^i$. The corresponding codeword $y = y_0 \dots y_{n-1}$ is the concatenation of evaluations of p over distinct elements of GF(q) $\setminus \{0\}$, e.g. $y_i = p(\alpha^i)$, $i = 0, \dots, n-1$, where α is a primitive element of GF(q).

There exist efficient algorithms for decoding Reed-Solomon codes. For instance, the classical Berlekamp-Massey algorithm [13], which is capable of correcting $t = \lfloor (d-1)/2 \rfloor$ errors, where d is the minimum distance of the code. However, for previously known algorithms t/n never exceeds 0.5 by much, not even for very low rates. To be useful for our purpose this bound on t is too low. Sudan's algorithm, on the other hand, corrects 100% of the errors asymptotically (for rates going towards 0).

The decoding problem as treated by Sudan may be stated as the following: Given integers n, k, and e. Furthermore n pairs $\{(x_i, y_i)\}_{i=1}^n$, $x_i, y_i \in$ GF(q) with pairwise distinct x_i. Compute all polynomials $p_1, \dots, p_m$ of degree $k - 1$ such

that for every $j = 1, 2, \ldots, m$, the following holds: $p_j(x_i) = y_i$ for at least $(n-e)$ values of $i = 1, \ldots, n$. It is not hard to see the similarity between this decoding problem and the problem of discovering a probabilistic relation $y = p(x)$ between plaintext x and ciphertext y.

The algorithm given by Sudan [18] solves this problem in polynomial time for values of e very close to n. The main result of Sudan [17] is the following:

Theorem 7. *For every ε and κ, the bounded distance decoding problem with parameters n, $k = \kappa n$, and $e = \epsilon(\kappa)n$ can be solved in polynomial time provided*

$$\varepsilon(\kappa) < 1 - \frac{1}{1+\rho_k} - \frac{\rho_k}{2}\kappa, \text{ where } \rho_\kappa = \left\lfloor \sqrt{\frac{2}{\kappa} - \frac{1}{4}} - \frac{1}{2} \right\rfloor.$$

Here κ is the fraction of information bits per codeword and $\varepsilon(\kappa)$ is the corresponding error rate. Note that for small κ we have $\rho_\kappa \approx \sqrt{2/\kappa}$, and in this case the right hand side of the inequality is approximately $1 - \sqrt{2\kappa}$.

Decoding beyond the packing radius is achieved by a very novel approach. Sudan's algorithm obtains a bivariate polynomial $Q(x, y)$ which is then factored into irreducibles. The error positions are then derived from the factorization and the received vector.

The following section shows how the error-correcting algorithm may be used to mount an attack.

4 Attack 1

Definition 8. *Let $a, b \in \mathbb{N}$. The (a, b)-weighted degree of a bivariate polynomial $Q(x, y) = \sum_{ij} q_{ij} x^i y^j$ is defined by*

$$\deg^{(ab)}(Q) = \max\{ia + jb | q_{ij} \neq 0\}.$$

The following algorithm is based on the modified Sudan's algorithm found in [4].

Attack 1:

- Input: n p/c-pairs $\{(x_i, y_i)\}_{i=1}^n$, $0 \leq \mu \leq 1$, $m \in \mathbb{N}$, such that $n > (2m)/(\mu^2)$.
- Output: All expressions $y - p(x)$ with $\deg(p) \leq m$ such that $y = p(x)$ holds with probability at least μ.
- Step A: Denote by $s_i(x, y)$ the i-th bivariate monomial in the $(1, m-1)$-weighted graded order. Let $Q(x, y) = \sum_{i=1}^{n+1} s_i(x, y)$ and let q_{ij} denote the coefficient of the monomial $x^i y^j$. Find a nonzero solution q_{ij} to the set of linear equations $Q(x_s, y_s) = 0$, $s = 1, \ldots, n$.
- Step B: Factor the polynomial $Q(x, y)$ into irreducibles over $\mathrm{GF}(q)[x, y]$.
- Step C: Output all factors $y - p(x)$ with $\deg(p) \leq m$ such that $p(x_i) = y_i$ for at least a fraction μ of $i = 1, \ldots, n$.

For a proof of Sudan's algorithm consult [17], [18], or [4]. The algorithm runs in polynomial time since there are efficient algorithms for solving linear equations and factoring polynomials [5].

As an optimization [8], note that it is possible to obtain from a bivariate polynomial factors on the form $y - p(x)$ by using a homomorphism from $\mathrm{GF}(q)[y]$ to $\mathrm{GF}(q_2)$ (for an appropriate power of q, q_2). Simply consider $Q(x, y) \in \mathrm{GF}(q)[x, y]$ as a polynomial in y from $\mathrm{GF}(q_2)[y]$ and then use, e.g., Berlekamp's algorithm [2] for factorization of univariate polynomials.

Theorem 9. *An (m, μ)-expressible cipher can be broken by Attack 1 using*

$$n = \frac{2m}{\mu^2} \tag{2}$$

plaintext/ciphertext pairs in time polynomial in n.

Proof. The theorem follows directly by rewriting Sudan's formula (setting $m = k$, $\mu = 1 - \varepsilon$ and approximating $\lfloor \sqrt{2/\kappa + 1/4} - 1/2 \rfloor$ by $\sqrt{2/\kappa}$; κ is assumed to be near 0 since $k \ll n$).

Example 10. The cipher constructed in [15] by Knudsen and Nyberg is immune to differential and linear cryptanalysis. It falls for an attack using Sudan's algorithm.

The cipher is a Feistel network with round function $F_k(x) = d(f(e(x) + k))$ where $f : \mathrm{GF}(2^{33}) \to \mathrm{GF}(2^{33})$, $f(x) = x^3$, $k \in \mathrm{GF}(2^{33})$, $e : \mathrm{GF}(2^{32}) \to \mathrm{GF}(2^{33})$ is a function which extends its argument by concatenation with an affine combination of the input bits, and $d : \mathrm{GF}(2^{33}) \to \mathrm{GF}(2^{32})$ discards one bit from the argument. As in [9] we call this cipher $\mathcal{KN}$. The following equations describe the cipher

$$\begin{aligned} C_i^L &= C_{i-1}^R \\ C_i^R &= F_{K_i}(C_{i-1}^R) + C_{i-1}^L. \end{aligned}$$

The plaintext is (C_0^L, C_0^R) and the ciphertext is the concatenation of C_r^R and C_r^L. Note that because of the extend and discard functions, one round cannot be written as a low-degree polynomial over $\mathrm{GF}(q)$.

Define the following variant $\mathcal{KN}'$ taking inputs $(C_0^L, C_0^R) \in \mathrm{GF}(2^{33})^2$ and having outputs $(C_r^R, C_r^L) \in \mathrm{GF}(2^{33})^2$:

$$\begin{aligned} D_0^L &= d(C_0^L) \\ D_0^R &= d(C_0^R) \\ D_i^L &= D_{i-1}^R \\ D_i^R &= F_{K_i}(D_{i-1}^R) + D_{i-1}^L \\ C_r^L &= e(D_r^L) \\ C_r^R &= e(D_r^R), \end{aligned}$$

In other words, $\mathcal{KN}'$ is simply $\mathcal{KN}$ preceded by discard operations and followed by extend operations. Clearly, if we can break $\mathcal{KN}'$ then we can also break $\mathcal{KN}$. Consequently, we proceed by attacking $\mathcal{KN}'$.

Consider yet another cipher $\mathcal{PURE}$ defined by the purely algebraically given round function $\tilde{F} : \mathrm{GF}(2^{33}) \to \mathrm{GF}(2^{33})$, $\tilde{F}_k(x) = f(x+k)$, $f(x) = x^3$. I.e.,

$$C_i^L = C_{i-1}^R$$
$$C_i^R = \tilde{F}_{K_i}(C_{i-1}^R) + C_{i-1}^L.$$

Again, the ciphertext is the concatenation of C_r^R and C_r^L. Here $C_i^L, C_i^R \in \mathrm{GF}(2^{33})$. Essentially, $\mathcal{PURE}$ is the same cipher as $\mathcal{KN}'$ but without the extend/discard functions that ruin the algebraic simplicity. Now keep the right half of the plaintext C_0^R constant and express the right half of the ciphertext C_r^L as a polynomial of the left half of the plaintext C_0^L. In the original proposal, $\mathcal{KN}$ has $r = 6$ rounds. Assume that this holds for $\mathcal{KN}'$ and $\mathcal{PURE}$ as well. Then the output polynomial of the right half has degree $3^{(6-2)} = 81$ due to the cipher's simple algebraic structure (C_0^L passes through $r-2$ instances of $\tilde{F}$ before "becoming" C_r^L). This implies that $\mathcal{PURE}$ can be broken by the interpolation attack which was exactly what was done in [9].

Assume that the position of the discarded bit is the same as the position of the extended bit. In this case, given the same inputs, the outputs from the round functions F and $\tilde{F}$ of $\mathcal{KN}'$ and $\mathcal{PURE}$, respectively, will agree with probability $\frac{1}{2}$ (when the extension function correctly "guesses" the missing bit). In other words, $e(d(f(x)))$ is $(3, \frac{1}{2})$-expressible over $\mathrm{GF}(2^{33})$. Consequently, given identical inputs with right halves fixed, the right halves of the outputs of the two ciphers $\mathcal{KN}'$ and $\mathcal{PURE}$ will agree on a fraction of $2^{-(6-2)} = 1/16$ of the possible plaintexts (we assume that the inputs to each round are uncorrelated).

Now we can use Thm. 9. We have $m = 81$ and $\mu = 1/16$. Consequently, using Sudan's algorithm we need at least

$$n = \frac{2 \times 81}{\left(\frac{1}{16}\right)^2} \approx 40000 < 2^{16}$$

pairs (x_i, y_i) to successfully discriminate random samples from p/c-pairs.

Combining Prop. 3 and Thm. 9 we can calculate the maximum number of rounds possible to break. Solving

$$\frac{2 \cdot 3^{r-2}}{1/\left(2^{r-2}\right)^2} \leq 2^{32}$$

for integer solutions gives a maximum of $r = 10$ rounds for which the cipher is breakable using at most 2^{32} p/c-pairs. Using higher order differentials (h.o.d.) as in [9], one can break only 7 rounds of $\mathcal{KN}$. Additionally, the h.o.d. approach depends on the extension bit being an affine combination of the input bits; this implies that the output bits of the round function may be considered as evaluations of quadratic polynomials of the input bits. Our attack does not rely on this assumption.

5 Attack 2

In [1], Ar et al. shows how to obtain low-degree relations $p(x,y) = 0$ that hold on a non-negligible number of elements of some set $\{(x_i, y_i)\}_{i=1,\ldots,n}$ (given the relations exist). Here we present a slightly weaker theorem which has the advantage of a shorter and less involved proof. In order to prove that the attack works, we need the following lemmas.

Lemma 11. Bézout's Theorem. *Let $P(x,y), Q(x,y) \in \mathrm{GF}(q)[x,y]$ be polynomials in two variables over $\mathrm{GF}(q)$. If the polynomials have no common factors, then the number of common zeros is at most $\deg P \cdot \deg Q$, where* deg *denotes total degree.*

For a proof consult [7].

Lemma 12. *Let $f(a,b)$ denote the number of bivariate polynomials in $\mathrm{GF}(q)[x,y]$ with degree a in x and degree b in y. Similarly, let $\Phi(a,b)$ count the number of irreducibles among these polynomials. Then*

$$\Phi(a,b) = (1 - q^{-a}) f(a,b) + O(aq^{ab}),$$

where the constant in the O-term depends on q and a.

A proof is found in [3]. Restated we get the following.

Lemma 13. *Let $p(x,y)$ be a random bivariate polynomial over $\mathrm{GF}(q)$ of degree a in x and degree b in y. Then the probability of $p(x,y)$ being irreducible satisfies*

$$\mathrm{Prob}[p(x,y) \text{ is irreducible}] \geq 1 - q^{-\max\{a,b\}}.$$

In other words, nearly all bivariate polynomials are irreducible.

Attack 2:

- Input: μ, m, n p/c-pairs $\{(x_i, y_i)\}$, where $n > (2m/\mu)^2$.
- Output (with high probability): All probabilistic links $p(x,y)$ with $\deg(p) \leq m$ satisfying $\mathrm{Prob}[p(x,y) = 0] \geq \mu$.
- Step A: Let $t_i(x,y)$ denote the i-th monomial in the graded order. Let $Q(x,y) = \sum_{i=1}^{n+1} t_i(x,y)$ and let q_{ij} be the coefficient of the monomial $x^i y^j$. Find a nonzero solution q_{ij} to the set of linear equations $Q(x_s, y_s) = 0$, $s = 1, \ldots, n$.
- Step B: Factor $Q(x,y)$. Output all factors of degree less than m.

Theorem 14. *Given a block cipher, assume that there exists a probabilistic relation $p(x,y) = 0$ with $\deg(p) \leq m$ between plaintext x and ciphertext y which holds for a fraction μ of the possible plaintexts.*

Then the cipher can be broken by Attack 2 using at most

$$n = \left(\frac{2m}{\mu}\right)^2$$

plaintext/ciphertext pairs and time polynomial in n.

Proof. First, we show that $Q(x,y)$ has non-constant factors if there is a probabilistic low degree relation between input and output. Assume that

$$p(x,y) = 0 \text{ with probability } \mu \tag{3}$$

for some $p(x,y) \in \mathrm{GF}(q)[x,y]$ with $\deg p \leq m$. In addition, assume that

$$n > \left(\frac{2m}{\mu}\right)^2. \tag{4}$$

We have $Q(x_i,y_i) = 0$ for n pairs (x_i,y_i). Of these $m = \mu n$ pairs have the additional property that $p(x,y) = 0$. Consequently, the number of common zeros of p and Q is at least m. We also have $\deg p \leq m$ and because of the way we constructed Q, we have $\deg Q \leq 2\sqrt{n}$. Then due to (4) we have $\deg Q \cdot \deg p < m$. By Bézout's theorem this means that p and Q have a common factor. Since $p \neq Q$, the polynomial $Q(x,y)$ must be reducible. In addition, p has a high probability of being irreducible implying that p is most probably one of the obtained factors.

Secondly, to prove that the algorithm outputs nothing when the pairs are truly random (implying that no probabilistic relations exist) it suffices to show that Q is "random". Recall that a random bivariate polynomial has very slim chances of being reducible. Also notice that the construction of Q is a matter of solving n linear equations of n unknown variables (assuming Q is to be normalized). In fact, we may choose the pairs (x_i,y_i) such that we obtain any assignment of coefficients $q_{ij} \in \mathrm{GF}(q)$. As a consequence, given random input we may assume that Q is random and therefore irreducible with high probability.

The algorithm runs in polynomial time since there exists efficient algorithms for solving sets of linear equations and factoring polynomials.

6 Comments

It is possible to break block ciphers which are probabilistically expressible as low degree polynomials faster than exhaustion of the key space. This fact should lead to new design criteria. Clearly, to thwart these attacks it is not enough that round functions have high boolean complexity. Likewise, good properties against differential and linear attacks are no guarantee either. In fact, many almost perfect non-linear functions should be avoided exactly because they are too simple algebraically. At least, they should not be the only ingredients of a strong block cipher. It remains to carry out analysis of existing block ciphers and discover whether they are susceptible to these new attacks.

Although both attacks run in polynomial time, in practice the running time may be substantial. Step A dominates the complexity; more precisely, solving linear equations using, e.g., simple Gaussian elimination gives time complexity $O(n^3)$. Factorization of bivariate polynomials over a finite field has complexity $O(n \log q)^{O(1)}$, see [5]. The memory requirement (to hold the system of linear equations) is proportional to the square of the number of unknown coefficients

q_{ij} in $Q(x, y)$, i.e. $O(n^2)$. It might be possible to improve these complexities with elimination algorithms suited for a particular purpose.

For both algorithms to work, there must be included in the n pairs at least μn pairs that satisfy the polynomial relation. Statistically, for n randomly chosen p/c-pairs this holds approximately 50% of the time since there is a fraction μ of good pairs among all possible p/c-pairs. To obtain a higher success rate one can simply use sufficiently many more p/c-pairs.

In this paper we have considered only bivariate relations. However, Sudan et al. describe extensions to several variables. This might be useful for ciphers where there is no natural correspondence between input or output and GF(q), e.g., for DES a more natural input domain would be GF(2)^w instead of GF(2^w) leading to polynomial relations of the form $y_i = p(x_1, \ldots, x_{64})$ or $q(x_1, \ldots, x_{64}, y_1, \ldots, y_{64}) = 0$.

Notice that for Prop. 6 to work, the discriminator does not need to explicitly output the probabilistic relation; it just has to state whether one exists. This fact might make it possible to construct even better attacks. In the error-correction setting, this resolves to computing whether a received word is closer to the set of codewords than some given distance.

More recently, Sudan [19] has improved his algorithm by requiring each pair (x, y) to appear as a root in Q with multiplicity greater than 1. This makes it possible to correct even more errors when decoding. In our case, the new results imply that the factor of 2 in Eq. (2) becomes close to 1.

Finally, note that both attacks are very well suited for (nearly-)black box analysis since no structure on the block cipher is assumed except the correspondence between plaintext/ciphertext and the elements of GF(q).

7 Acknowledgements

Thanks to Tom Høholdt for fruitful discussions and for mentioning Sudan's results in the first place.

References

1. Sigal Ar, Richard J. Lipton, Ronitt Rubinfeld, and Madhu Sudan. Reconstructing Algebraic Functions from Mixed Data, *Proceedings of the 33rd Annual IEEE Symposium on Foundations of Computer Science*, 1992, pp. 503–512. To appear SIAM Journal on Computing.
2. Elwyn R. Berlekamp. Factoring Polynomials over Large Finite Fields. *Mathematics of Computation*, pp. 713, vol. 24, no. 111, 1970.
3. Leonard Carlitz. The Distribution of Irreducible Polynomials in Several Indeterminates II. *Canadian Journal of Mathematics* 17:261-266, 1965.
4. Weishi Feng and Richard E. Blahut. On Decoding Reed-Solomon Codes Beyond the Packing Radii. Preprint. Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, Nov., 1997.
5. Joachim von zur Gathen and Erich Kaltofen. Factoring multivariate polynomials over finite fields. *Math. Comput.*, 45:251-261, 1985.

6. Carlo Harpes, Gerhard G. Kramer, and James L. Massey. A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-up Lemma. *Eurocrypt '95*, Lectures Notes in Computer Science, Springer, 1995.
7. Robin Hartshorne. *Algebraic Geometry.* Springer-Verlag, New York, 1977.
8. Tom Høholdt. Private communication.
9. Thomas Jakobsen and Lars R. Knudsen. The Interpolation Attack on Block Ciphers. *Fast Software Encryption IV*, Lecture Notes in Computer Science, Springer, Haifa, 1997.
10. Xueijia Lai. Higher order derivatives and differential cryptanalysis. In *Proc. "Symposium on Communication, Coding and Cryptography", in honor of James L. Massey on the occasion of his 60'th birthday*, Feb. 10–13, 1994, Monte-Verita, Ascona, Switzerland, 1994.
11. Xuejia Lai and James L. Massey. A Proposal for a New Block Encryption Standard, *Advances in Cryptology - Eurocrypt '90 Proceedings*, Springer-Verlag, Berlin, 1991, pp. 389–404.
12. Xuejia Lai, James L. Massey, and Sean Murphy. Markov ciphers and differential cryptanalysis. *Advances in Cryptology, Proceedings Eurocrypt '91*, LNCS 547, D. W. Davies, Ed., Springer-Verlag, 1991, pp. 17–38.
13. Florence J. MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, 1977.
14. Mitsuru Matsui. Linear cryptanalysis for DES cipher. *Lecture Notes in Computer Science, 765* (1994), 386–397. (Advances in Cryptology - EUROCRYPT '93.)
15. Kaisa Nyberg and Lars R. Knudsen. Provable Security Against a Differential Attack. *Journal of Cryptology*, vol. 8, no. 1, 1995.
16. Ronald L. Rivest. The RC5 encryption algorithm. In Bart Preneel, editor, *Fast Software Encryption: Second International Workshop*, Lecture Notes in Computer Science, vol. 1008, pp. 86-96, Leuven, Belgium, Springer-Verlag, Published 1995.
17. Madhu Sudan. Decoding Reed Solomon Codes beyond the Error-Correction Diameter. *Proc. 35th Annual Allerton Conference on Communication, Control and Computing*, University of Illinois at Urbana-Champaign, 1997.
18. Madhu Sudan. Decoding of Reed Solomon Codes beyond the Error-Correction Bound. *Journal of Complexity*, 13(1):180-193, March 1997.
19. Madhu Sudan. Preprint. May 1998.