Root Finding Interpolation Attack

Kaoru Kurosawa, Tetsu Iwata, and Viet Duong Quang

Department of Communication and Integrated Systems,
Tokyo Institute of Technology,
2–12–1 O-okayama, Meguro-ku, Tokyo 152–8552, Japan
{kurosawa,tez,viet}@ss.titech.ac.jp

Abstract. In this paper, we first show that there are *several equivalent* keys for $t+1$ chosen plaintexts if the degree of the reduced cipher is $t-1$. This is against the claim by Jakobsen and Knudsen. We also derive an upper bound on the number of equivalent last round keys for $t+1$ chosen plaintexts. We further show an efficient method which finds all the equivalent keys by using Rabin's root finding algorithm. We call our attack *root finding interpolation attack*

Keywords: Block cipher, interpolation attack, root finding algorithm, resultant.

1 Introduction

Consider a Feistel type block cipher of block size $2n$ with a round function $F(K,x)$. For a fixed key K, $F(K,x)$ can be viewed as a polynomial $f_K(x)$ in x over $\mathrm{GF}(2^n)$. The interpolation attack [4] succeeds if $\deg f_K(x)$ is small for any K and the number of rounds is not large. More precisely, suppose that the degree of the reduced cipher is $t-1$, where the degree of the reduced cipher will be defined in Definition 2.1. Then

1. Jakobsen and Knudsen claimed that the last round key K_m can be recovered from $t+1$ chosen plaintexts (see [4, Theorem 3]).
2. They used exhaustive search to find K_m.

On the other hand, given a polynomial $f(x)$ over $\mathrm{GF}(p)$, Berlekamp proposed a probabilistic algorithm of finding a root $\alpha \in \mathrm{GF}(p)$ of $f(x)=0$ for any odd prime p [1]. Rabin generalized Berlekamp's algorithm to any finite fields [8]. In Rabin's algorithm, the expected number of bit operations to find a root of $f(x)=0$ over $\mathrm{GF}(2^n)$ is

$$O(n^2 dL(d)L(n)),$$

where $d=\deg f(x)$ and $L(n)=\log n \times \log\log n$.

In this paper, we first show that for $t+1$ chosen plaintexts, there are *several equivalent* keys. This is against the claim by Jakobsen and Knudsen [4, Theorem 3]. We also derive an upper bound on the number of equivalent last round keys for $t+1$ chosen plaintexts.

D.R. Stinson and S. Tavares (Eds.): SAC 2000, LNCS 2012, pp. 303–314, 2001.

We next show an efficient method which finds all the equivalent last round keys K_m. We call our attack *root finding interpolation attack* because it uses Rabin's root finding algorithm [8]. By using more than $t+1$ chosen plaintexts, we can uniquely determine K_m.

Further, Jakobsen and Knudsen claimed that the number of necessary chosen plaintexts can be smaller than $t+1$ if they use the meet in the middle approach [4]. However, the number of equivalent keys increases if the number of chosen plaintexts decreases in general. Therefore, their claim cannot be justified. For this problem, we derive another upper bound on the number of equivalent last round keys for a certain number of chosen plaintexts which is less than $t+1$.

Related works: Youssef and Gong studied the effect of the choice of the irreducible polynomial defining GF(2^n) on $\deg f_K(x)$ and whether or not there exists a simple linear transformation on the input or output bits such that the resulting polynomial has a less degree [9].

The higher differential attack succeeds if the round function $F(K, x)$ can be expressed as a set of low degree Boolean functions [4]. Moriai et al. showed an improved higher differential attack for a 5 rounds CAST cipher in which K_m is computed by solving simultaneous linear equations [6].

2 Preliminaries

2.1 Notation

Consider an m round Feistel type block cipher with block size $2n$. Let $x = (x_L, x_R)$ denote the plaintext, where $x_L = (x_1, \ldots, x_n)$ and $x_R = (x_{n+1}, \ldots, x_{2n})$. Similarly, let $y = (y_L, y_R)$ denote the ciphertext. Let

$$C_0^L \stackrel{\triangle}{=} x_L \text{ and } C_0^R \stackrel{\triangle}{=} x_R \ .$$

The round function F operates as follows.

$$\begin{cases} C_i^L = C_{i-1}^R \ , \\ C_i^R = F(K_i, C_{i-1}^R) + C_{i-1}^L \ , \end{cases} \tag{1}$$

where K_i denotes the i-th round key. The ciphertext $y = (y_L, y_R)$ is given by (C_m^R, C_m^L). See Fig. 1.

2.2 Reduced Cipher Assumption

We say that:

1. (C_{m-1}^R, C_{m-1}^L) is the reduced ciphertext and
2. (C_{m-2}^R, C_{m-2}^L) is the second reduced ciphertext, respectively.

Define

$$\tilde{y} = (\tilde{y}_L, \tilde{y}_R) \stackrel{\triangle}{=} (C_{m-1}^R, C_{m-1}^L)$$

$$\hat{y} = (\hat{y}_L, \hat{y}_R) \stackrel{\triangle}{=} (C_{m-2}^R, C_{m-2}^L).$$

See Fig. 1.

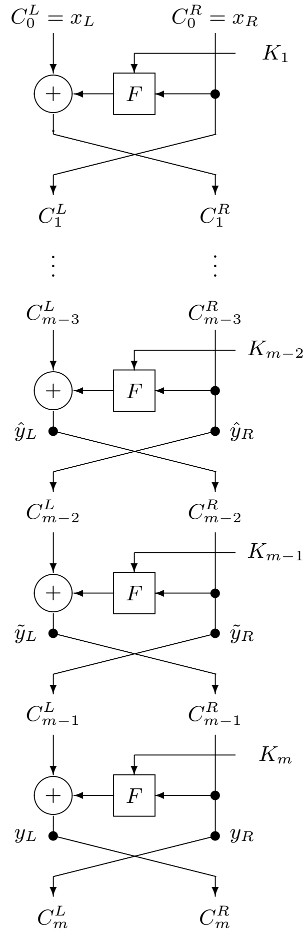

Fig. 1. The m round Feistel cipher

Definition 2.1. *Fix the right half of a plaintext x_R as $x_R = 0$. Fix the key of the block cipher arbitrarily. Then we say that:*

1. *A block cipher satisfies the reduced cipher assumption of degree $t-1$ if the right half $\tilde{y}_R$ of the reduced ciphertext can be expressed as*

$$\tilde{y}_R = f_1(x_L) \tag{2}$$

for some polynomial $f_1(x)$ over $GF(2^n)$ such that $\deg f_1(x) \le t-1$.

2. *A block cipher satisfies the second reduced cipher assumption of degree $u-1$ if the right half $\hat{y}_R$ of the second reduced ciphertext can be expressed as*

$$\hat{y}_R = f_2(x_L) \tag{3}$$

for some polynomial $f_2(x)$ over $GF(2^n)$ such that $\deg f_2(x) \le u-1$.

2.3 Lagrange Interpolation

Let Q be a field. Given $2t$ elements $x_1, \ldots, x_t, y_1, \ldots, y_t \in Q$, where the x_is are distinct. Define

$$f(x) = \sum_{i=1}^{t} \lambda_i(x) y_i, \tag{4}$$

where

$$\lambda_i(x) = \prod_{1 \le j \le t, j \ne i} \frac{x - x_j}{x_i - x_j}.$$

Then $f(x)$ is the only polynomial over Q of degree at most $t-1$ such that $f(x_i) = y_i$ for $i = 1, \ldots, t$. Eq.(4) is known as the *Lagrange interpolation formula.*

3 Root Finding Algorithm over GF(2^n)

Given a polynomial $h(x)$ of degree d with coefficients in GF(2^n), Rabin showed an efficient probabilistic polynomial time algorithm which computes a root of $h(x) = 0$ in GF(2^n) if such a root does exist [8].

First compute

$$h_1(x) = \gcd(h(x), x^{2^n-1} - 1).$$

If $h_1(x) = 1$, then $h(x)$ has no roots in GF(2^n). In general,

$$h_1(x) = (x - \alpha_1) \cdots (x - \alpha_k),\ k \le d,$$

where the α_i are the pairwise different roots in GF(2^n) of $h(x) = 0$.

On the other hand, the trace function is defined as

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

For any $\alpha \in$ GF(2^n), it is known that

$$\mathrm{Tr}(\alpha) = 0 \text{ or } 1.$$

Rabin first proved the following proposition

Proposition 3.1. *For any fixed $\alpha_1 \ne \alpha_2 \in$ GF(2^n), choose $r \in$ GF(2^n) randomly. Then*

$$\Pr(\mathrm{Tr}(r\alpha_1) \ne \mathrm{Tr}(r\alpha_2)) = \frac{1}{2}.$$

Rabin next showed the following root finding algorithm.

Let $h_0(x) = h_1(x)$.

Step 1. If $\deg h_0(x) = 1$, then we have found a root. Otherwise goto step 2.
Step 2. Choose $r \in$ GF(2^n) randomly. Compute

$$h_r(x) = \gcd(h_0(x), \mathrm{Tr}(rx)).$$

Step 3. If $h_r(x) = 1$ or $h_0(x)$, goto step 2. Otherwise, let

$$h_0(x) := \begin{cases} h_r(x) & \text{if } \deg h_r(x) \leq \frac{1}{2} \deg h_0(x) \\ h_0(x)/h_r(x) & \text{otherwise.} \end{cases}$$

Goto Step 1.

From Proposition 3.1, it holds that

$$\Pr\left[0 < \deg h_r(x) < \deg h_1(x)\right] \geq \frac{1}{2}.$$

Therefore, it can be shown that [8] the expected number of bit operations is

$$O(n^2 dL(d)L(n)),$$

where

$$L(n) = \log n \times \log \log n.$$

4 Equivalent Keys and Root Finding Interpolation Attack

In this section, we first show that for $t + 1$ chosen plaintexts, there are *several equivalent* keys. This is against the claim by Jakobsen and Knudsen [4, Theorem 3]. We also derive an upper bound on the number of equivalent last round keys for $t + 1$ chosen plaintexts.

We next show an efficient method which finds all the equivalent keys. We call our attack *root finding interpolation attack* because it uses Rabin's root finding algorithm [8]. By using more than $t + 1$ chosen plaintexts, we can uniquely determine K_m.

For a plaintext $(x_L, x_R) = (x_i, 0)$, let $(y_{L,i}, y_{R,i})$ denote the ciphertext, $(\tilde{y}_{L,i}, \tilde{y}_{R,i})$ denote the reduced ciphertext and $(\hat{y}_{L,i}, \hat{y}_{R,i})$ denote the second reduced ciphertext.

4.1 Key Equation

In this subsection, we derive a key equation

$$h(K_m) = 0$$

in K_m such that $\deg h(K_m) \leq d$, where d is given below.

Definition 4.1. *We say that the round function F satisfies K polynomial assumption of degree d if for any fixed x, there exists a polynomial g_x with* $\deg g_x(K) \leq d$ *such that*

$$F(K, x) = g_x(K).$$

Suppose that there exists a block cipher which satisfies the *reduced cipher assumption of degree* $t-1$. Further, without loss of generality, we can assume that there exists d such that the block cipher satisfies K *polynomial assumption of degree* d.

First by using the Lagrange formula, $f_1(x)$ of eq.(2) can be expressed as

$$f_1(x) = \lambda_1(x)f_1(x_1) + \cdots + \lambda_t(x)f_1(x_t)$$

for some polynomials $\lambda_1(x), \ldots, \lambda_t(x)$, where each $\lambda_i(x)$ is determined by x_1, $\ldots, x_t$. Then we have

$$f_1(x_{t+1}) = \lambda_1(x_{t+1})f_1(x_1) + \cdots + \lambda_t(x_{t+1})f_1(x_t)$$

for $x = x_{t+1}$. Substituting eq.(2) into the above equation yields that

$$\tilde{y}_{R,t+1} = \lambda_1(x_{t+1})\tilde{y}_{R,1} + \cdots + \lambda_t(x_{t+1})\tilde{y}_{R,t} \tag{5}$$

On the other hand, from eq.(1), it holds that

$$\tilde{y}_{R,i} = F(K_m, y_{R,i}) + y_{L,i}. \tag{6}$$

Substitute eq.(6) into eq.(5). Then we have

$$\begin{aligned} &F(K_m, y_{R,t+1}) + y_{L,t+1} \\ &\quad = \lambda_1(x_{t+1})(F(K_m, y_{R,1}) + y_{L,1}) + \cdots + \lambda_t(x_{t+1})(F(K_m, y_{R,t}) + y_{L,t}) \end{aligned} \tag{7}$$

The above equation is rearranged as

$$h(K_m) = 0 \tag{8}$$

for some polynomial of K_m over $\mathrm{GF}(2^n)$ such that

$$\deg h(K) \le d$$

from K *polynomial assumption of degree* d. We call eq.(8) the key equation. (This equation is not redundant. That is, we cannot reduce $\deg h(K_m)$.)

4.2 Equivalent Keys

Jakobsen and Knudsen claimed that the last round key K_m can be recovered from $t+1$ chosen plaintexts in [4, Theorem 3]. However, eq.(8) implies that there are d or less equivalent keys. Now we have proved the following theorem.

Theorem 4.1. *Suppose that there exists a block cipher which satisfies the reduced cipher assumption of degree* $t-1$ *and* K *polynomial assumption of degree* d*. Then for* $t+1$ *chosen plaintexts, there are* d *or less equivalent last round keys.*

In fact, the interpolation attack must require more than $t+1$ chosen plaintexts to uniquely determine K_m. If the round function $F(K, x)$ is not algebraically constructed, the situation is worse because d is usually large. In this case, there are many equivalent keys for $t+1$ chosen plaintexts and the interpolation attack will require many chosen plaintexts to uniquely determine K_m.

4.3 Root Finding Interpolation Attack

We propose an attack which efficiently finds all the equivalent keys K_m by solving eq.(8) by using Rabin's algorithm of Sec.3. By using more than $t+1$ chosen plaintexts, we can uniquely determine K_m. We call this attack *root finding interpolation attack*.

First suppose that $t+1$ chosen plaintext/ciphertext pairs are available such that the plaintexts are $(x_1, 0), \ldots, (x_{t+1}, 0)$ and the ciphertexts are $(y_{L,1}, y_{R,1})$, $\ldots, (y_{L,t+1}, y_{R,t+1})$. Then

Step 1. Compute the coefficients of $h(K_m)$ of eq.(8) from $x_1, \ldots, x_{t+1}$ and $(y_{L,1}, y_{R,1}), \ldots, (y_{L,t+1}, y_{R,t+1})$. Especially, $\lambda_i(x)$ is determined by $x_1, \ldots, x_t$ though the Lagrange interpolation formula.

Step 2. Solve eq.(8) by using Rabin's algorithm of Sec.3. Then we obtain d or less equivalent keys K_m.

Next suppose that some extra (chosen plaintext, ciphertext) pairs are available. Then the set of equivalent keys is made smaller and we can finally uniquely determine K_m. An alternative way is as follows. Obtain two key equations $h_i(K_m) = 0$ for $i = 1, 2$ from $t+2$ chosen plaintexts. Compute $\gcd(h_1(K_m), h_2(K_m))$. If K_m is uniquely determined from the gcd, then we have done. Otherwise, execute the same procedure for more chosen plaintexts.

5 On the Meet in the Middle Approach

Jakobsen and Knudsen also claimed that the number of necessary chosen plaintexts can be smaller than $t+1$ if they use the meet in the middle approach [4]. However, the number of equivalent keys increases if the number of chosen plaintexts decreases in general. Therefore, their claim cannot be justified.

In this section, we derive an upper bound on the number of equivalent last round keys for certain number of chosen plaintexts which is less than $t+1$.

Suppose that there exists a block cipher which satisfies the *second reduced cipher assumption of degree* $u-1$ and K *polynomial assumption of degree* d. Then from $u+2$ chosen plaintexts, we first derive two equations on (K_{m-1}, K_m) such that

$$H_1(K_{m-1}, K_m) = 0,$$
$$H_2(K_{m-1}, K_m) = 0.$$

We next compute the resultant

$$h(K_m) \overset{\triangle}{=} R(H_1, H_2)$$

of H_1 and H_2 which yields that $\deg h(K_m) \leq 2d^3$. The above equation means that there are $2d^3$ or less equivalent last round keys for $u+2$ chosen plaintexts.

Finally, we can find all the equivalent keys by solving $h(K_m) = 0$ by the Rabin's algorithm.

5.1 Resultant [10]

Let

$$A(x) = \sum_{i=0}^{d} a_i x^i$$
$$B(x) = \sum_{i=0}^{e} b_i x^i$$

be two polynomials over a field Q.

Define

$$R(A,B) = \det \left| \begin{array}{cccccc} a_d & a_{d-1} & \cdots & a_0 & & \\ & a_d & a_{d-1} & \cdots & a_0 & \\ & & \ddots & & \ddots & \\ b_e & b_{e-1} & \cdots & b_0 & & \\ & b_e & b_{e-1} & \cdots & b_0 & \\ & & \ddots & & \ddots & \end{array} \right| \begin{array}{l} \left.\vphantom{\begin{array}{c}1\\1\\1\end{array}}\right\} e \\ \left.\vphantom{\begin{array}{c}1\\1\\1\end{array}}\right\} d \end{array}$$

We say that $R(A,B)$ is the resultant of $A(x)$ and $B(x)$.

Proposition 5.1. *$A(x)$ and $B(x)$ have a common root in Q if and only if*

$$R(A,B) = 0.$$

5.2 Key Equation

First by using the Lagrange formula, $f_2(x)$ of eq.(3) can be expressed as

$$f_2(x) = \delta_1(x) f_2(x_1) + \cdots + \delta_u(x) f_2(x_u)$$

for some polynomials $\delta_1(x), \ldots, \delta_u(x)$, where each $\delta_i(x)$ is determined by x_1, $\ldots, x_u$. Then we have

$$f_2(x_{u+1}) = \delta_1(x_{u+1}) f_2(x_1) + \cdots + \delta_u(x_{u+1}) f_2(x_u)$$

for $x = x_{u+1}$. Substituting eq.(3) into the above equation yields that

$$\hat{y}_{R,u+1} = \delta_1(x_{u+1}) \hat{y}_{R,1} + \cdots + \delta_u(x_{u+1}) \hat{y}_{R,u} \tag{9}$$

On the other hand, from eq.(1), it holds that

$$\begin{aligned} \hat{y}_{R,i} &= F(K_{m-1}, \tilde{y}_{R,i}) + \tilde{y}_{L,i} \\ &= F(K_{m-1}, F(K_m, y_{R,i}) + y_{L,i}) + y_{R,i}. \end{aligned} \tag{10}$$

Substitute eq.(10) into eq.(9). Then we have

$$H_1(K_{m-1}, K_m) = 0$$

such that

$$H_1(K_{m-1}, K_m) = \sum_{i=0}^{d} a_i(K_m)K_{m-1}^i$$
$$\deg a_i(K_m) \leq d^2$$

from K polynomial assumption.

Similarly for $x = x_{u+2}$, we have

$$H_2(K_{m-1}, K_m) = 0$$

such that

$$H_2(K_{m-1}, K_m) = \sum_{i=0}^{d} b_i(K_m)K_{m-1}^i$$
$$\deg b_i(K_m) \leq d^2$$

Finally, let

$$h(K_m) \overset{\triangle}{=} R(H_1, H_2),$$

where $R(H_1, H_2)$ is the resultant of H_1 and H_2. From Proposition 5.1, it holds that

$$h(K_m) = 0$$

since H_1 and H_2 have a common root. Further, we can see that

$$\deg h(K) \leq 2d^3$$

5.3 Equivalent Keys

From the previous subsection, we obtain the following theorem.

Theorem 5.1. *Suppose that there exists a block cipher which satisfies the second reduced cipher assumption of degree $u-1$ and K polynomial assumption of degree d. Then for $u+2$ chosen plaintexts, there are $2d^3$ or less equivalent last round keys.*

5.4 Root Finding Resultant Attack

We propose an attack such as follows which we call *root finding resultant attack.*

First suppose that $u+2$ chosen plaintext/ciphertext pairs are available such that the plaintexts are $(x_1, 0), \ldots, (x_{u+2}, 0)$ and the ciphertexts are $(y_{L,1}, y_{R,1})$, $\ldots, (y_{L,u+2}, y_{R,u+2})$. Then

Step 1. Compute the coefficients of H_1 and H_2 from $x_1, \ldots, x_{u+2}$ and $(y_{L,1}, y_{R,1})$, $\ldots, (y_{L,u+2}, y_{R,u+2})$.

Step 2. Compute $h(K_m) = R(H_1, H_2)$.

Step 3. Solve $h(K_m) = 0$ by using Rabin's algorithm of Sec.3. Then we obtain $2d^3$ or less equivalent keys K_m.

Next suppose that some extra (chosen plaintext, ciphertext) pairs are available. Then the set of equivalent keys is made smaller and we can finally uniquely determine K_m. We can also have an alternative method similarly to Sec.4.3.

6 Example

The m round $\mathcal{PURE}$ cipher [4] is defined by letting

$$F(K, x) = (K + x)^3$$

over GF(2^{32}).

Lemma 6.1. *In eq.(4),*

$$\lambda_1(x) + \cdots + \lambda_t(x) = 1.$$

Proof. $f(x) = 1$ is the only polynomial over Q of degree at most $t - 1$ such that $f(x_i) = 1$ for $i = 1, \ldots, t$. Therefore, from eq.(4), we have

$$1 = \lambda_1(x) + \cdots + \lambda_t(x).$$

Q.E.D.

Corollary 6.1. *The m round $\mathcal{PURE}$ cipher has two or less equivalent last round keys for $3^{m-3} + 2$ chosen plaintexts.*

Proof. Let $t - 1 = 3^{m-3}$ and $d = 3$. Then Theorem 4.1 tells us that there are $d = 3$ or less equivalent last round keys for $t + 1 = 3^{m-3} + 2$ chosen plaintexts. However, in this case, eq.(7) is written as follows.

$$\begin{aligned}&(K_m + y_{R,t+1})^3 + y_{L,t+1}\\ &\quad = \lambda_1(x_{t+1})((K_m + y_{R,1})^3 + y_{L,1}) + \cdots + \lambda_t(x_{t+1})((K_m + y_{R,t})^3 + y_{L,t}).\end{aligned}$$

By rearranging the above equation, we obtain the key equation $h(K_m)$ such that

$$\deg h(K_m) = 2$$

because the coefficient of K_m^3 is canceled from lemma 6.1. This implies that there are two or less equivalent last round keys.

Q.E.D.

The proposed attack computes all the equivalent keys K_m by solving the quadratic equation $h(K_m) = 0$ over GF(2^{32}). By using one more chosen plaintext, we can uniquely determine K_m.

On the contrary, Jakobsen and Knudsen claimed that the interpolation attack needs $3^{m-3} + 2$ chosen plaintexts to recover K_m.

Corollary 6.2. *The m round $\mathcal{PURE}$ cipher has* 54 *or less equivalent last round keys for* $3^{m-4}+3$ *chosen plaintexts.*

Proof. Let $u-1=3^{m-4}$ and $d=3$. Then Theorem 5.1 tells us that there are $2d^3=54$ or less equivalent last round keys for $u+2=3^{m-4}+3$ chosen plaintexts. Q.E.D.

7 Summary

In this paper, we first showed that for $t+1$ chosen plaintexts, there are several equivalent last round keys if the degree of the reduced cipher is $t-1$. This is against the claim by Jakobsen and Knudsen on interpolation attack [4, Theorem 3]. We also derived an upper bound on the number of equivalent last round keys for $t+1$ chosen plaintexts.

We next showed an efficient method which finds all the equivalent last round keys K_m. We call our attack *root finding interpolation attack* because it uses Rabin's root finding algorithm [8]. By using more than $t+1$ chosen plaintexts, we can uniquely determine K_m.

The number of equivalent keys increases if the number of chosen plaintexts decreases in general. For this problem, we derived another upper bound on the number of equivalent last round keys for a certain number of chosen plaintexts which is less than $t+1$.

As an example, we showed that the m round $\mathcal{PURE}$ cipher has two or less equivalent last round keys for $3^{m-3}+2$ chosen plaintexts and 54 or less equivalent last round keys for $3^{m-4}+3$ chosen plaintexts. The proposed attack efficiently computes all the equivalent keys K_m by solving a key equation $h(K_m)=0$ over GF(2^{32}) by using Rabin's root finding algorithm. By using more chosen plaintext, we can uniquely determine K_m.

It will be interesting if we can extend our method to the probabilistic interpolation attack [3] which succeeds even if $F(K,x)$ is approximated by a low degree polynomial.

References

1. E.R.Berlekamp. Factoring polynomials over large finite fields. In *Math. Comput.*, vol. 24, pp. 713–735, 1970.
2. E.Biham and A.Shamir. Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag, 1993.
3. T.Jakobsen. Cryptanalysis of block ciphers with probabilistic non-linear relations of low degree. In *Advances in Cryptology — CRYPTO' 98 Proceedings*, volume 1462 of *Lecture Notes in Computer Science*, pages 212–222, Springer-Verlag, 1998.
4. T.Jakobsen and L.R.Knudsen. The interpolation attack on block ciphers. In *Fast Software Encryption*, volume 1267 of *Lecture Notes in Computer Science*, pages 28–40, Springer-Verlag, January 1997.
5. M.Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology — EUROCRYPT' 93 Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397, Springer-Verlag, 1993.

6. S.Moriai, T.Shimoyama and T.Kaneko. Higher order differential attack of a CAST cipher. Proc. of FSE '98, LNCS 1372, pp.17–32, (1998)
7. K.Nyberg and L.R.Knudsen. Provable security against a differential attack. In *Journal of Cryptology*, volume 8, number 1, pages 27–37, Winter 1995.
8. M.Rabin. Probabilistic algorithms in finite fields. SIAM Journal on Computing, vol.9, no.2, pp.273–280 (1980)
9. A.M.Youssef and G.Gong. On the interpolation attacks on block ciphers. Preproc. of FSE 2000, (2000)
10. R.Zippel. Effective polynomial computation. Kluwer Academic Publishers (1993)