Integral Cryptanalysis
(Extended abstract)

Lars Knudsen[1] ⋆ and David Wagner[2]

[1] Dept. of Mathematics, DTU, Building 303, DK-2800 Lyngby, Denmark
lars@ramkilde.com
[2] University of California Berkeley, Soda Hall, Berkeley, CA 94720, USA
daw@cs.berkeley.edu

Abstract. This paper considers a cryptanalytic approach called integral cryptanalysis. It can be seen as a dual to differential cryptanalysis and applies to ciphers not vulnerable to differential attacks. The method is particularly applicable to block ciphers which use bijective components only.
Keywords: cryptanalysis, block ciphers, integrals, MISTY.

1 Introduction

The last three decades have seen considerable progress in understanding the basic operating principles of block ciphers. One of the most significant advances was the introduction in 1990 of differential cryptanalysis [3]. In differential cryptanalysis, one considers the propagation of differences between (pairs of) values.

In this paper, we consider a cryptanalytic technique which considers the propagation of sums of (many) values. This approach can thus be seen as a dual to differential cryptanalysis [3]. A number of these ideas have been exploited before in specific scenarios, but in this paper we unify and extend previous work in a single consistent framework, and we propose the name *integral cryptanalysis* for this set of techniques.

Integrals have a number of interesting features. They are especially well-suited to analysis of ciphers with primarily bijective components. Moreover, they exploit the simultaneous relationship between many encryptions, in contrast to differential cryptanalysis where one considers only pairs of encryptions. Consequently, integrals apply to a number of ciphers not vulnerable to differential cryptanalysis. These features have made integrals an increasingly popular tool in recent cryptanalysis work, and this motivates our systematic study of integrals.

We begin by formulating integral cryptanalysis in a general group-theoretic setting and develop a consistent notation for expressing integral attacks. We also introduce an important extension to previous work, the *higher-order integral attack*. See Section 2.

⋆ Part of this author's work was done while visiting University of California San Diego on leave from the Department of Informatics, University of Bergen, Norway supported by the Norwegian Research Council

Table 1. Summary of some of our cryptanalytic results. For MISTY, all results are key-recovery attacks of the full cipher (including the FL functions). "Gen. Feistel" are key-recovery attacks of the generalised Feistel networks [26] with 64-bit blocks and bijective 8-bit S-boxes. All attacks use chosen plaintexts.

Cipher	(rounds)	Complexity [Data]	[Time]	Comments
MISTY1	(4)	2^{20}	2^{89}	see [19] (previously known)
MISTY1	(4)	$2^{22.25}$	2^{45}	see [20] (previously known)
MISTY1	(4)	2^{38}	2^{62}	see [19] (previously known)
MISTY1	(4)	25	2^{27}	integrals (new)
MISTY1	(5)	2^{34}	2^{48}	integrals (new)
MISTY2	(5)	2^{20}	2^{89}	see [19] (previously known)
MISTY2	(5)	2^{38}	2^{62}	see [19] (previously known)
MISTY2	(4)	9	2^{55}	integrals (new)
MISTY2	(6)	2^{34}	2^{71}	integrals (new)
Gen. Feistel	(13)	$2^{9.6}$	2^{32}	basic integral (new)
Gen. Feistel	(14)	$2^{10.6}$	2^{56}	basic integral (new)
Gen. Feistel	(14)	2^{16}	2^{24}	second-order integral (new)
Gen. Feistel	(15)	$2^{17.6}$	2^{40}	second-order integral (new)
Gen. Feistel	(16)	$2^{18.6}$	2^{64}	second-order integral (new)
Gen. Feistel	(16)	$2^{33.6}$	2^{56}	fourth-order integral (new)
Gen. Feistel	(17)	$2^{34.6}$	2^{80}	fourth-order integral (new)
Gen. Feistel	(17)	$2^{49.6}$	2^{72}	sixth-order integral (new)

In the main body of the paper, we first explain the well-known attacks on Square, Rijndael, Crypton (see Section 3), using our new concepts and notation, then we apply these techniques to a number of other ciphers: MISTY (Section 4), Nyberg's generalized Feistel networks (Section 5), see Table 1 for a summary of some of these results. Many of these attacks illustrate our new notion of higher-order integrals and its utility for cryptanalysis. Finally, we discuss how to extend these techniques to non-word-oriented ciphers (Section 6) and how to combine integrals with interpolation attacks (Section 7), we draw attention to some related work (Section 8), and we conclude the paper (Section 9). Due to page constraints we did not include our results on Skipjack. These can be found in the full version of this paper.

In this paper, a time complexity of n means that the time of an attack corresponds to performing n encryptions of the underlying block cipher.

2 Fundamentals of integral cryptanalysis

Let $(G, +)$ be a finite abelian group of order k. Consider the product group $G^n = G \times \ldots \times G$, that is, the group with elements of the form $v = (v_1, \ldots, v_n)$ where $v_i \in G$. The addition of G^n is defined component-wise, so that $u + v = w$ holds for $u, v, w \in G^n$ just when $u_i + v_i = w_i$ for all i.

Let S be a multiset of vectors. An integral over S is defined as the sum of all vectors in S. In other words, the integral is $\int S = \sum_{v \in S} v$, where the summation is defined in terms of the group operation for G^n. (For a multiplicative group this would usually be called a "product" instead.)

In integral cryptanalysis, n will represent the number of words in the plaintext and ciphertexts, and m denotes the number of plaintexts and ciphertexts considered (at a time). Typically, $m = k$ (recall that k is defined as the order of G, i.e., $k = |G|$), the vectors $v \in S$ represent the plaintext and ciphertexts, and $G = GF(2^s)$ or $G = Z/kZ$. In an attack, one tries to predict the values in the integrals after a certain number of rounds of encryption. For this purpose it is advantageous to distinguish between the three cases: where all ith words are equal; are all different; or sum to a certain value predicted in advance. Let $S \subseteq G^n$ be as before, and consider some fixed index i. We consider these cases.

$$v_i = c \qquad \text{for all } v \in S \tag{1}$$

$$\{v_i : v \in S\} = G \tag{2}$$

$$\sum_{v \in S} v_i = c' \tag{3}$$

where $c, c' \in G$ represent some known values that are fixed in advance.

Let us consider the typical case where $m = k$, that is, the number of vectors in the set S equals the number of elements in the considered group. If all ith words are equal then clearly the ith word in the integral will take the value of the neutral element of G (Lagrange's theorem). Furthermore, there is a result from group theory which allows us to predict the integral in the case when all ith words are different; it allows us to characterize the sum of all elements in G [11, Problem 2.1, p. 116].

Theorem 1. *Let $(G, +)$ be a finite abelian additive group, and let $H = \{g \in G : g + g = 0\}$ be the subgroup of elements of order 1 or 2. Write $s(G)$ for the sum $\sum_{g \in G} g$ of all the elements of G. Then $s(G) = \sum_{h \in H} h$. Moreover $s(G) \in H$, i.e., $s(G) + s(G) = 0$.*

Thus for $G = GF(2^s)$ we get $s(G) = 0$ and for Z/mZ we get $s(Z/mZ) = m/2$ when m is even or 0 when m is odd. There is an analogue for multiplicatively written groups.

Theorem 2. *Let $(G, *)$ be a finite abelian multiplicative group and let $H = \{g \in G : g * g = 1\}$ be the subgroup of elements of order 1 or 2. Write $p(G)$ for the product $\prod_{g \in G} g$ of all the elements of G. Then $p(G) = \prod_{h \in H} h$. Moreover $p(G) \in H$, i.e., $p(G) * p(G) = 1$.*

For example, when $G = (Z/pZ)^*$ where p is prime, $p(G) = -1$ (Wilson's theorem).

Thus, in all the above three cases (1), (2), and (3) we have a tool to predict the value of the sum of all words.

In differential cryptanalysis over a group G, one typically considers differences defined in terms of the subtraction or division, e.g. $dx = x' - x$ for an additive group or $dx = x' \cdot x^{-1}$ for a multiplicative group. We claim that the right operation for integrals is addition or multiplication.

Suppose the cipher computes $w_j = u_j + v_j$ where u_j, v_j, w_j are intermediate values. Suppose also the integral predicts that the words u_j and v_j are of the forms (1), (2), or (3). What can we say about the words w_j? We can at least say that $\sum w_j = \sum u_j + \sum v_j$, where the sum is taken over some set of encryptions. Thus, if the sum of the words u_j and v_j are known, the sum of the words w_j can be determined. Moreover, if the words u_j are all equal and the words v_j are all different, then the words w_j are all different, and so on.

A good cipher also contains nonlinear components, or nonlinear S-boxes. Assume that at some point in the cipher the function f is applied to a word, i.e., $v_j = f(u_j)$. Clearly, if the words u_j are all equal (of the form (1)), then so are the words v_j. Also, if f is a permutation (bijection) and if the words u_j are all different (of the form (2)), then so are the words v_j.

By analogy to higher-order differentials (see next section), we define higher-order integrals. Consider a set $\tilde{S} = S_1 \cup \ldots \cup S_s$ made up of s sets of vectors, where each S_i forms an integral. Then clearly, if one can determine the sum of the elements of S_i for each i, then one can also determine the sum of all vectors in $\tilde{S}$. Suppose the words in a cipher can take m values each. Consider a set of m vectors (representing a set of plaintexts) which differ only in one particular word. The sum over the vectors of this set is called a first-order integral. Consider next a set of m^d vectors which differ in d components, such that each of the m^d possible values for the d-tuple of values from these components occurs exactly once. The sum of this set is called an dth-order integral.

Let us introduce the following symbols for words in an integral. For a first-order integral, the symbol '$\mathcal{C}$' (for "Constant") in the ith entry, means that the values of all ith words in the collection of texts are equal. The symbol '$\mathcal{A}$' (for "All") means that all words in the collection of texts are different, and the symbol '$\mathcal{S}$' (for "Sum") means that the sum of all ith words can be predicted. Finally, we will write '?' when the sum of words can not be predicted.

For dth-order integrals we use $\mathcal{C}$ and ? as before, and we use the notation $\mathcal{A}^d$ to denote that the corresponding component participates in a dth-order integral. If we assume that one word can take m different values, then $\mathcal{A}^d$ means that in the integral the particular word takes all values exactly m^{d-1} times. We shall use $\mathcal{A}$ as a short notation for $\mathcal{A}^1$. To express further the interdependencies between particular words we introduce the following notation: The terms $\mathcal{A}_i^d$ mean that in the integral the string concatenation of all words with subscript i take the m^d values exactly once.

Integrals can be probabilistic just like differentials [3]. However, all integrals for the specific ciphers given in this paper are of probability one.

Comparison with other concepts

First we note that integrals are somewhat similar to truncated differentials [16, 15, 18]. In the latter, one often is only interested in whether the words in a pair are equal or different [2]. Thus integrals restricted to pairs of texts with only the values 0 and $\mathcal{A}$ coincide with such truncated differentials. Integrals, though, can also represent texts with the value $\mathcal{S}$; truncated differentials cannot, which may make integrals a more powerful tool in some cases.

Also, integrals are somewhat similar to higher-order differentials. Let $(G, +)$ be an Abelian group. For a function $f : G \rightarrow G$ the first-order derivative [21] at the point a is defined as $f_a(x) = f(x + a) - f(x)$. This is the definition of a differential or characteristic that is traditionally used in cryptanalysis. One can extend the definition of differentials to higher orders. One defines [21] the ith-order derivative of f at the point $a_1, \ldots, a_i$ as follows:

$$f_{a_1,\ldots,a_i}(x) = f_{a_i}(f_{a_1,\ldots,a_{i-1}}(x)). \tag{4}$$

As an example, a third-order derivative is:

$$\begin{aligned} f_{a,b,c}(x) = {} & f(x+a+b+c) - f(x+a+b) - f(x+b+c) - f(x+a+c) + \\ & f(x+a) + f(x+b) + f(x+c) - f(x) \end{aligned}$$

Thus for general groups the higher-order derivatives (or higher-order differentials) are not the same as integrals, since in an integral one would consider the sum of all elements in a set. In groups of characteristic two, an sth-order differential is the exclusive-or of all 2^s different words, and therefore also an integral. But where for integrals one distinguishes between the three cases (1), (2), and (3), for higher-order differentials only the value of (4) is used.

Higher-order differentials have traditionally been used in cryptanalytic attacks on ciphers which consist of subfunctions with a low algebraic degree. For groups with characteristic two it holds that an sth-order differential of a function of algebraic degree s is a constant (and consequently an $(s + 1)$st-order differential of a function of algebraic degree s is zero).

To sum up, in some cases integrals contain both truncated and higher-order differentials, but there are cases where integrals can be specified for more rounds than either of the other two. On the other hand, in contrast to truncated and higher-order differentials, integrals do not seem to apply as well to ciphers using non-bijective S-boxes/subcomponents.

In the remainder of this paper we give examples of integrals for a variety of ciphers.

3 Square, Rijndael, and Crypton

In *FSE'97* an integral attack was given on the block cipher Square [5]. This attack can be applied also to the ciphers Rijndael [7, 9] and Crypton [8]. All three ciphers are 128-bit block ciphers operating on bytes. The sixteen bytes are arranged in a 4×4 matrix. One round of the ciphers consists of the addition of a subkey, a substitution of each byte, and a linear transformation, MixColumn, which modifies the four bytes in a column in the matrix. In the following we shall apply integral cryptanalysis to Rijndael only. Due to the similarity between these

Table 2. A 3-round (first-order) integral for Rijndael, where $\mathcal{S} = 0$

$$\begin{array}{|c|c|c|c|}\hline \mathcal{A}&\mathcal{C}&\mathcal{C}&\mathcal{C}\\\hline \mathcal{C}&\mathcal{C}&\mathcal{C}&\mathcal{C}\\\hline \mathcal{C}&\mathcal{C}&\mathcal{C}&\mathcal{C}\\\hline \mathcal{C}&\mathcal{C}&\mathcal{C}&\mathcal{C}\\\hline\end{array} \longrightarrow \begin{array}{|c|c|c|c|}\hline \mathcal{A}&\mathcal{C}&\mathcal{C}&\mathcal{C}\\\hline \mathcal{A}&\mathcal{C}&\mathcal{C}&\mathcal{C}\\\hline \mathcal{A}&\mathcal{C}&\mathcal{C}&\mathcal{C}\\\hline \mathcal{A}&\mathcal{C}&\mathcal{C}&\mathcal{C}\\\hline\end{array} \longrightarrow \begin{array}{|c|c|c|c|}\hline \mathcal{A}&\mathcal{A}&\mathcal{A}&\mathcal{A}\\\hline \mathcal{A}&\mathcal{A}&\mathcal{A}&\mathcal{A}\\\hline \mathcal{A}&\mathcal{A}&\mathcal{A}&\mathcal{A}\\\hline \mathcal{A}&\mathcal{A}&\mathcal{A}&\mathcal{A}\\\hline\end{array} \longrightarrow \begin{array}{|c|c|c|c|}\hline \mathcal{S}&\mathcal{S}&\mathcal{S}&\mathcal{S}\\\hline \mathcal{S}&\mathcal{S}&\mathcal{S}&\mathcal{S}\\\hline \mathcal{S}&\mathcal{S}&\mathcal{S}&\mathcal{S}\\\hline \mathcal{S}&\mathcal{S}&\mathcal{S}&\mathcal{S}\\\hline\end{array}$$

three ciphers, the attack applied to the other two ciphers is quite similar to the attack on Rijndael [8].

Consider a collection of 256 texts, which have different values in one byte and equal values in all other bytes. Then it follows that after two rounds of encryption the texts take all 256 values in each of the sixteen bytes, and that after three rounds of encryption the sum of the 256 bytes in each position is zero [5]. Also, note that there are 16 such integrals since the position of the non-constant byte in the plaintexts can be in any of the sixteen bytes. The integral is illustrated in Table 2. This integral can be used to attack four rounds of Rijndael (or Square or Crypton) with small complexity (note that the final round is special and does not include MixColumn) counting over one key byte at a time. Simply guess a key byte and compute byte-wise backwards to check if the sum of all 256 values is zero.

The attack can be extended to five rounds using the same integral over the first three rounds. Guess one key byte in the fifth round and four in the fourth round, in total five key bytes at a time. The attack can be further extended to six rounds using the same integral as above but used now from the second round and onwards. Here one chooses a collection of 2^{32} plaintexts, such that for each guess of four key bytes in the first round, one can find a collection of 256 ciphertexts after one round of encryption which form an integral. Guess further one key byte in the sixth round and four in the fifth round, in total nine bytes.

The following observation was made which led to an improvement in the running time of the attack [9]. Instead of guessing four key bytes in the first round, one uses all 2^{32} texts in the analysis. The main observation is that the 2^{32} plaintexts together form 2^{24} copies of the above integrals (starting in the second round). Since the text in each integral sums to zero in any byte after the fourth round, so does the sum of all 2^{32} texts. This attack finds less key bits than the original Square attack of *FSE'97* [5], but the running time is greatly improved. (The improvement is in the key-search part of the attack). Table 3 depicts this four-round fourth-order integral.

4 MISTY

Integrals can be used to attack some reduced-round variants of Matsui's MISTY1 and MISTY2 [24]. We refer to the MISTY specifications [24] for the description of these ciphers and for the notation used in the following.

In earlier work, Sakurai and Zheng noted the following property of the MISTY2 round function [28]. Let $F(x, y)$ denote the left half of the output of

Table 3. A four-round fourth-order integral for Rijndael with 2^{32} texts.

$$
\begin{array}{|c|c|c|c|}\hline \mathcal{A}_0^4 & \mathcal{C} & \mathcal{C} & \mathcal{C} \\ \hline \mathcal{C} & \mathcal{A}_0^4 & \mathcal{C} & \mathcal{C} \\ \hline \mathcal{C} & \mathcal{C} & \mathcal{A}_0^4 & \mathcal{C} \\ \hline \mathcal{C} & \mathcal{C} & \mathcal{C} & \mathcal{A}_0^4 \\ \hline \end{array}
\longrightarrow
\begin{array}{|c|c|c|c|}\hline \mathcal{A}_0^4 & \mathcal{C} & \mathcal{C} & \mathcal{C} \\ \hline \mathcal{A}_0^4 & \mathcal{C} & \mathcal{C} & \mathcal{C} \\ \hline \mathcal{A}_0^4 & \mathcal{C} & \mathcal{C} & \mathcal{C} \\ \hline \mathcal{A}_0^4 & \mathcal{C} & \mathcal{C} & \mathcal{C} \\ \hline \end{array}
\longrightarrow
\begin{array}{|c|c|c|c|}\hline \mathcal{A}_0^4 & \mathcal{A}_0^4 & \mathcal{A}_0^4 & \mathcal{A}_0^4 \\ \hline \mathcal{A}_1^4 & \mathcal{A}_1^4 & \mathcal{A}_1^4 & \mathcal{A}_1^4 \\ \hline \mathcal{A}_2^4 & \mathcal{A}_2^4 & \mathcal{A}_2^4 & \mathcal{A}_2^4 \\ \hline \mathcal{A}_3^4 & \mathcal{A}_3^4 & \mathcal{A}_3^4 & \mathcal{A}_3^4 \\ \hline \end{array}
\longrightarrow
\begin{array}{|c|c|c|c|}\hline \mathcal{A}^4 & \mathcal{A}^4 & \mathcal{A}^4 & \mathcal{A}^4 \\ \hline \mathcal{A}^4 & \mathcal{A}^4 & \mathcal{A}^4 & \mathcal{A}^4 \\ \hline \mathcal{A}^4 & \mathcal{A}^4 & \mathcal{A}^4 & \mathcal{A}^4 \\ \hline \mathcal{A}^4 & \mathcal{A}^4 & \mathcal{A}^4 & \mathcal{A}^4 \\ \hline \end{array}
\longrightarrow
$$

$$
\begin{array}{|c|c|c|c|}\hline \mathcal{S} & \mathcal{S} & \mathcal{S} & \mathcal{S} \\ \hline \mathcal{S} & \mathcal{S} & \mathcal{S} & \mathcal{S} \\ \hline \mathcal{S} & \mathcal{S} & \mathcal{S} & \mathcal{S} \\ \hline \mathcal{S} & \mathcal{S} & \mathcal{S} & \mathcal{S} \\ \hline \end{array}
$$

three rounds of MISTY2 on plaintext $\langle x, y\rangle$. They observe that F has the form $F(x, y) = f(x) \oplus g(y)$, where f and g are some key-dependent bijective mappings. Consequently, if we pick sets S, T each containing two arbitrary 32-bit values, then we will have

$$\sum_{\langle x,y\rangle \in S\times T} F(x, y) = 0. \tag{5}$$

We note that this may be viewed as a three-round integral for MISTY2.

This provides an efficient chosen-plaintext attack on four rounds of MISTY2. Choosing S', T' with $|S'| = |T'| = 3$ gives us four independent ways to choose S, T with $S \subset S'$, $T \subset T'$, $|S| = |T| = 2$, and thus this use of 'structures' yields four independent integrals of the above form. For each integral, we guess KO_{44}, KI_{43}, KO_{43}, and $KI_{421} \oplus \text{truncate}(KI_{422})$ (55 bits in all), and peel off enough of the last round to check that the 17th through 23rd bits of the input to the last round XOR to zero (a 7-bit condition on each of the four integrals). Guesses that survive this filtering phase can be further tested by guessing KI_{422} and checking an additional 9-bit condition. In this way we expect that all incorrect guesses will be eliminated, and then the remainder of the key may be recovered easily. In summary, this breaks four rounds of MISTY2 with work comparable to 2^{55} trial encryptions and just 9 chosen plaintexts. A known-plaintext variant would need 2^{33} texts and comparable work.

Also, there is an attack on six rounds of MISTY2, which works as follows. Consider the integral $\langle \mathcal{A}, \mathcal{C}\rangle$. After four rounds we have $\langle \mathcal{S}, \mathcal{S}\rangle$, where $\mathcal{S} = 0$. Note that texts with sum to zero at the input to the function FL, also sum to zero after FL, in other words, there is a probability one integral throught the FL function. After five rounds we have $\langle \mathcal{S}, ?\rangle$. Using Kühn's [19, page 328] alternative MISTY description, one sees that in a 6-round version, one can compute backwards from the ciphertext through $FO6$ to the 16 rightmost bits (which has the value $\mathcal{S}$ in the integral) by guessing at most 50 key bits. Note here that the key AKO_{63} in Kühns representation need not be guessed. It can be moved to the end of the first round of $FO6$ (in the right half) by exoring it to AKO_{64} and to AKO_{65}. With one structure of 2^{32} chosen plaintexts, 2^{34} of the 2^{50} possible values of the target key bits would be left suggested, thus with four structures one can expect only one suggested and correct value of 50 key bits. In total the attack needs 2^{34} chosen plaintext and has a time complexity of 2^{80}.

The attack on six rounds of MISTY2 can be further improved. Consider the second FI-function in $FO6$ (in Kühns reprensentation). The nine-bit key AKI_{ij} can be moved up before the "truncate step" if it is added to the left half (truncated to 7 bits) of the output of FI. Then in $FO6$ it should be added to the seven most significant bits of both halves of the output of $FO6$. In this version of an attack one would count on only 41 key bits. The disadvantage is that one can test on only seven data bits. So with one structure 2^{34} keys are left suggested. One can now either check on a few other structures or introduce the "remaining" 9 key bits from the before mentioned attack and run that attack. As an example, run the improved attack on two structures, which leaves 2^{27} out of 2^{41} possible values of the target key bits. Then run the first attack, with nine additional unknown key bits, which leaves 2^{18} out of 2^{50} possible values. With four structures, in total 2^{34} chosen plaintexts, the time complexity of the attack is 2^{71}.

We can also attack five rounds of MISTY1 using a related idea. There is a four-round integral $\langle \mathcal{C}, \mathcal{A} \rangle \to \langle ?, \mathcal{S} \rangle$. We collect four instances of this integral with 2^{34} chosen texts and apply a 1-R attack [3]. Note that $FO5$ has the same structure as three MISTY2 rounds, so it has a Sakurai-Zheng property [28]. In other words, we can write bits 1–7 of the right half of the block just before applying $FO5$ as a function $f_{KO_{51}}(C) \oplus g_{KO_{52}}(C) \oplus k'$ of the ciphertext C, for some functions f, g and some key-dependent constant k'. Our integral predicts that this value will sum to zero when summed over each integral of 2^{32} ciphertexts, or equivalently,

$$\sum_i f_{KO_{51}}(C_i) = \sum_i g_{KO_{52}}(C_i).$$

This gives a 7-bit condition for each integral, so taken together our four integrals will yield a 28-bit condition. We note that one can use a meet-in-the-middle technique to find solutions to this equation efficiently: we enumerate all 2^{16} possibilities for $\sum_i f_{KO_{51}}(C_i)$, then merge this list with the 2^{16} possibilities for $\sum_i g_{KO_{52}}(C_i)$, and their intersection yields candidates for KO_{51} and KO_{52}. Then further key material can be recovered by using guesses at KI_{512} and KI_{522} to check a 16-bit condition on each integral, and so on. These ideas allow us to break five rounds of MISTY1 with 2^{34} chosen plaintexts and work comparable to 2^{48} trial encryptions. Many tradeoffs between the time and data complexities are possible.

There is also an attack on four rounds of MISTY1 (without $FL5, FL6$) with very low data complexity. We apply the Sakurai-Zheng property twice: once to predict the sum of four outputs of $FO2$, and then a second time in the 1-R analysis to recover key material from $FO4$. We choose 25 plaintexts whose left halves are fixed and whose right halves range over the values $\langle x, y \rangle \in S' \times S'$, for some set S' containing five arbitrary 16-bit values. This choice ensures that we find 16 quadruples S, T of inputs to $FO2$ that each satisfy the conditions of Equation 5 (having survived $FL2$ without disruption, thanks to the choice of plaintexts). Thus, the XOR of the left half of the output of $FO2$ over each such quadruple will be zero. This propagates to the input of the fourth round undisturbed by $FL3$ at each bit position where KL_{32} has a one bit. We obtain a 7-bit condition on each quadruple of ciphertexts,

$$\mathrm{truncate}(KL_{32}) \wedge \sum_i f_{KO_{41}}(C_i) = \mathrm{truncate}(KL_{32}) \wedge \sum_i g_{KO_{42}}(C_i).$$

Guessing truncate(KL_{32}) and applying meet-in-the-middle techniques will typically let us find KO_{41} and KO_{42} with about 2^{30} simple steps of computation. The attack can be continued as before by guessing KI_{412}, KI_{422}, and the rest of KL_{32}. We expect that these techniques will give an attack on four rounds of MISTY1 that, for most keys, uses about 25 chosen plaintexts and takes time comparable to 2^{27} trial encryptions.

5 Generalised Feistel networks

Nyberg has proposed a *generalised Feistel network* with block size $2nd$ bits [26]. We briefly describe the construction here. Let $X_0, \ldots, X_{2n-1}$ be the inputs to one round of the cipher. Given n S-boxes $F_0, \ldots, F_{n-1}$, where $F_i : \{0,1\}^d \to \{0,1\}^d$, and n round keys $K_0, \ldots, K_{n-1}$, the output of the round $Z_0, \ldots, Z_{2n-1}$ is defined as follows:

$$\begin{aligned} Y_i &= X_i \oplus F_i(K_i \oplus X_{2n-1-i}), \text{ for } i = 0, \ldots, n-1 \\ Y_i &= X_i \text{ for } i = n, \ldots, 2n-1 \\ Z_i &= Y_{i-1} \text{ for } i = 0, \ldots, 2n-1, \end{aligned}$$

where all indices are computed modulo $2n$. The integrals and attacks to follow are independent of the key schedule. Therefore, it is assumed that all round keys are independent and chosen uniformly at random.

As a special example, Nyberg considers the cases where the S-boxes are bijective. In this case the probabilities of differentials can be upper bounded to p^{2n} where p is the probability of a non-trivial differential through the S-boxes. With $n = 4$ and $d = 8$ there are S-boxes for which $p = 2^{-6}$ and the probabilities of all differentials over 12 rounds are bounded by 2^{-48}. Also, the probabilities of linear hulls over 12 rounds can be bounded by 2^{-48} [26].

For the above network with $n = 4$, $d = 8$, and bijective S-boxes, there exists an integral of probability one over eleven rounds using only 256 texts. Consider Table 4. It follows that for the integral where all first words are different, and where all other words are held constant, the sum of the first words after eleven rounds of encryption is zero. Thus, for a 12-round version of this cipher it is trivial to find eight bits of the key in the last round using the above integral by simply computing backwards from the ciphertexts to the outputs of the eleventh round. Also, a 13-round version can be attacked using the integral by computing backwards from the ciphertext to the eleventh round output by guessing only three key bytes. In this case, the attack must be repeated a few times to be

Table 4. An 11-round integral with 256 texts for the generalized Feistel cipher with $n = 4$, $d = 8$ and using bijective S-boxes. In the integral $\mathcal{S} = 0$.

Ciphertexts after round	$\mathcal{A}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$
1	$\mathcal{C}$	$\mathcal{A}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$
2	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{A}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$
3	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{A}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$
4	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{A}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$
5	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{C}$	$\mathcal{C}$
6	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{C}$
7	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{S}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$
8	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{S}$	?	$\mathcal{S}$	$\mathcal{A}$	$\mathcal{A}$
9	$\mathcal{A}$	$\mathcal{S}$	$\mathcal{S}$	?	?	?	$\mathcal{S}$	$\mathcal{A}$
10	$\mathcal{A}$	$\mathcal{S}$	?	?	?	?	?	$\mathcal{S}$
11	$\mathcal{S}$	?	?	?	?	?	?	?

able to uniquely determine the secret keys. This attack would run in total time approximately 2^{32} using $3 \cdot 2^8$ chosen texts. A 14-round and a 15-round version can be attacked by guessing a total of six respectively ten key bytes in a straight forward extension of the previous attack. These attacks would run in total times approximately 2^{56} respectively 2^{88} using $6 \cdot 2^8$ respectively $10 \cdot 2^8$ chosen texts. However, in these cases it is advantageous to use an integral of higher order. Consider the 13-round second-order integral in Table 5.

It follows by a closer look at the structure of the cipher that the values of the 16 bits of the first and second words after one round of encryption are a permutation of the 16-bit values of the first and eighth words of the plaintexts. Therefore by choosing 2^{16} plaintexts different only in the first and eighth words (counting from the left) one gets a collection of 2^8 integrals of the form in Table 4 this time starting from the second round. Therefore, one would expect to be able to determine the sum of the first words after 12 rounds. However, this integral goes one round further. To see this, consider Table 5. The question is why after nine rounds of encryption the fifth words sum to zero (the $\mathcal{S}$ after nine rounds of encryption in Table 5). It follows by simple observations that the 16-bit value $(x \mid y)$ consisting of the fifth (x) and sixth words (y) after five rounds of encryption is a permutation of the 16 varying bits in the plaintexts. Furthermore, the fourth word after seven rounds of encryption has the form $g_1(x)$ and the fifth word after seven rounds of encryption has the form $g_2(x) + g_3(y)$, for some bijective key-dependent functions g_i. Therefore, these 16 bits are a permutation of x and y and therefore also a permutation of the 16 varying bits in the plaintexts. This is illustrated in the integral where the two words are assigned the symbol $\mathcal{A}_4^2$. It then follows that the fifth words after eight rounds of encryption take all possible values equally many times. By similar arguments, it follows that the fourth and seventh words after rounds of encryption map one-to-one to the 16 varying bits in the plaintexts; therefore the fourth words after 8 rounds of encryption take all possible values equally many times. The

Table 5. A 13-round integral with 2^{16} texts for the generalised Feistel cipher with $n = 4$, $d = 8$ and using bijective S-boxes. In the integral $\mathcal{S} = 0$.

Ciphertexts after round	$\mathcal{A}_0^2$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{A}_0^2$
1	$\mathcal{A}_0^2$	$\mathcal{A}_0^2$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$
2	$\mathcal{C}$	$\mathcal{A}_0^2$	$\mathcal{A}_0^2$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$
3	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{A}_0^2$	$\mathcal{A}_0^2$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$
4	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{A}_0^2$	$\mathcal{A}_0^2$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$
5	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{A}_0^2$	$\mathcal{A}_0^2$	$\mathcal{C}$	$\mathcal{C}$
6	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{A}_1^2$	$\mathcal{A}_0^2$	$\mathcal{A}_1^2$	$\mathcal{A}_0^2$	$\mathcal{C}$
7	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{A}_3^2$	$\mathcal{A}_4^2$	$\mathcal{A}_4^2$	$\mathcal{A}_3^2$	$\mathcal{A}_2^2$	$\mathcal{A}_2^2$
8	$\mathcal{A}_2^2$	$\mathcal{A}_5^2$	$\mathcal{A}_5^2$	$\mathcal{A}_3^2$	$\mathcal{A}_4^2$	$\mathcal{A}_4^2$	$\mathcal{A}_3^2$	$\mathcal{A}_2^2$
9	$\mathcal{A}_2^2$	$\mathcal{A}_2^2$	$\mathcal{A}^2$	$\mathcal{A}^2$	$\mathcal{S}$	$\mathcal{A}_4^2$	$\mathcal{A}_4^2$	$\mathcal{A}^2$
10	$\mathcal{A}^2$	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$	?	$\mathcal{S}$	$\mathcal{A}_4^2$	$\mathcal{A}_4^2$
11	$\mathcal{A}_4^2$	$\mathcal{S}$	?	?	?	?	$\mathcal{S}$	$\mathcal{A}_4^2$
12	$\mathcal{A}_4^2$	$\mathcal{A}_4^2$	?	?	?	?	?	$\mathcal{S}$
13	$\mathcal{S}$	?	?	?	?	?	?	?

Table 6. A 14-round integral with 2^{32} texts for the generalised Feistel cipher with $n = 4$, $d = 8$ and using bijective S-boxes. In the integral $\mathcal{S} = 0$.

Ciphertexts after round	$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{A}^4$	$\mathcal{A}^4$
	...	...	...	...	...	...	...	...
14	$\mathcal{S}$	?	?	?	?	?	?	?

fact that both the fourth and fifth words after eight rounds of encryption take all possible values equally many times explains why the sum of the fifth words after nine rounds of encryption is zero. Finally we note that there are other ways of specifying interdependencies of the words in the integral of Table 5. As an example the symbols after six rounds of encryption could also be specified as

$$\mathcal{C}, \mathcal{C}, \mathcal{C}, \mathcal{A}_1^2, \mathcal{A}_1^2, \mathcal{A}_0^2, \mathcal{A}_0^2, \mathcal{C}.$$

One can find eight key bits of a 14-round version using the integral by simply computing backwards from the ciphertexts to the outputs of the thirteenth round. The time complexity of this attack is approximately 2^{24} using 2^{16} texts. A 15-round and a 16-round version can be attacked by guessing a total of three respectively six key bytes in a straight forward extension of the previous attack. These attacks would run in total times approximately 2^{40} respectively 2^{64} using $3 \cdot 2^{16}$ respectively $6 \cdot 2^{16}$ chosen texts. Clearly, the attacks using the second-order integral are much faster than the attacks using a first-order integral, but on the down side they require more chosen plaintexts.

Let us go one step further and consider the fourth-order integral of Table 6. This integral contains 2^{16} copies of the second-order integral of Table 5 but starting here from the second round and onwards. Therefore, one can determine (at least) the sum of the first words after 14 rounds of encryption. Using this integral there are attacks on a 15-round, 16-round and a 17-round version which run in total times approximately 2^{40}, 2^{56} respectively 2^{80} using 2^{32}, $3 \cdot 2^{32}$ respectively $6 \cdot 2^{32}$ chosen texts.

There exists a sixth-order integral over 15 rounds with a total of 2^{48} chosen texts. This would enable an attack on a 17-round version of total time complexity approximately 2^{72} using $3 \cdot 2^{48}$ chosen texts.

Finally we note that there are impossible differentials for the above ciphers. With $n = 4$ we have detected a 14-round differential of probability zero. A set of plaintexts which differ only in the first word will never result in ciphertexts (after 14 rounds of encryption) different in only the fourth words. The differential can be used to distinguish a 14-round version of the generalised Feistel network from a randomly chosen permutation using about 2^{50} chosen texts. For comparison the integral of Table 6 can be used to distinguish the cipher from a randomly chosen permutation using only 2^{32} chosen texts with good advantage.

6 DES

So far we have only considered round functions that break the block into several independent words and then operate only in a word-oriented fashion. However, this restriction is not always satisfied: in some ciphers—for example, DES—the round function operates on individual bits (not words) and the inputs to the S-boxes are correlated. In this more general case, our previous techniques for constructing integrals may not apply.

In this section we consider more general round functions. In particular, we show that the existence of integrals is not limited to word-oriented ciphers or to S-boxes whose inputs are independent. Since DES is a classic example where neighboring S-boxes in the same round are fed related inputs and where the round function works at the bit level, we will use the DES round function as a concrete example of how to build integrals for more general S-box networks.

As a starting example to illustrate the possibility of finding integrals on the DES round function F, we give a simple integral. Let the inputs to F take on values of the form $u_z = \langle z, z, z, z \rangle$, where z varies over all values in $\{0,1\}^8$. Then we claim that $\sum_z F(u_z) = 0$, i.e., the XOR of the corresponding 2^8 outputs of the F function will be zero. This fact will imply that the above structure of 2^8 texts yields an integral for one round of DES.

The proof of the claim requires a bit of knowledge about the form of the DES F function. Recall that the DES round function takes the form $F = P \circ S \circ E$ where $E : \{0,1\}^{32} \to \{0,1\}^{48}$ expands its input by duplicating some input bits, where $S : \{0,1\}^{48} \to \{0,1\}^{32}$ is composed of eight parallel S-boxes

$$S(x_1, \ldots, x_{48}) = \langle S_1(x_1, \ldots, x_6), \ldots, S_8(x_{43}, \ldots, x_{48}) \rangle$$

where each S-box has a corresponding map $S_i : \{0,1\}^6 \to \{0,1\}^4$, and where the bit-permutation P is irrelevant to our discussion. Also, the expansion function E

ensures that the inputs $\langle v_1, \ldots, v_6 \rangle, \langle w_1, \ldots, w_6 \rangle$ to any two consecutive S-boxes satisfy $v_5 = w_1$ and $v_6 = w_2$.

Now we can see why the above integral works. When the input to the F function is $\langle z, z, z, z \rangle$, the odd S-boxes receive $\langle z_8, z_1, \ldots, z_5 \rangle$ as input, and the even S-boxes receive $\langle z_4, \ldots, z_8, z_1 \rangle$. Note that each S-box takes on all 2^4 possible output values exactly four times if its input takes on each possible 6-bit input value exactly once. Consequently, if we focus on any one S-box, we see that its output will take on all 4-bit values exactly four times as we range over all possible choices of z, which means that these outputs will XOR to zero. Since this is true for each S-box, and since the P bit-permutation is linear with respect to XOR, we see that $\sum_z F(u_z) = 0$ (where the addition operation is the exclusive-or). This gives a simple integral for the F function containing 2^8 inputs.

There are more complicated integrals that use fewer input texts. For example, if we consider F-function inputs of the form

$$u = \langle d, e, f, a, b, e, f, c, d, a, b, e, f, c, d, a, b, e, f, c, d, a, b, e, f, c, d, a, b, e, f, c \rangle$$

where the 6-bit value $\langle a, b, c, d, e, f \rangle$ varies over all 2^6 possibilities, we find that $\sum F(u) = 0$. (The input to S_1 is $\langle c, d, e, f, a, b \rangle$ and hence takes on all possibilities exactly once; the input to S_2 is $\langle a, b, e, f, c, d \rangle$; and in general, the input to each S-box is a permutation of the 6 bits a, b, c, d, e, f.)

In fact, there even exist integrals containing only 2^5 inputs. We use the following property of the S-boxes: $S_i(w_1, \ldots, w_6)$ is a bijective function of $\langle w_2, \ldots, w_5 \rangle$ when w_1, w_6 are held fixed. With this observation, we consider inputs of the form

$$u = \langle a, b, c, d, e, a, b, c, d, a, b, e, c, a, b, d, e, a, b, c, d, a, e, b, c, d, e, a, b, c, d, e \rangle$$

where the 5-bit value $\langle a, b, c, d, e \rangle$ ranges over all 2^5 possibilities. This choice ensures that each S-box has an input pattern of the form $\langle i, j, k, l, m, i \rangle$ (where i, j, k, l, m represent some re-ordering of the bits a, b, c, d, e), and then the XOR of the corresponding 2^5 outputs will be zero, as required. We leave it as an open question to determine whether there exist integrals for the DES F function that use a smaller number of inputs.

We stress that we do not know of any way to use these integrals to mount an attack on more than a few rounds of DES. Thus, the main interest of these observations is likely to be in their motivational value: they show that it may be possible to find integrals even on fairly complicated round functions.

7 Integral-interpolation attacks

An interesting property of integrals is that they can be combined with interpolation attacks [13]. Consider a cipher whose first half may be covered by an integral and whose second half may be approximated using a low-degree polynomial. Suppose that we have a set of chosen plaintext/ciphertext pairs (P_i, C_i) following the integral, and let Z_i denote the corresponding intermediate values predicted by the integral. Assuming that the integral ends with an $\mathcal{S}$, we have

$\sum_i Z_i = 0$. Suppose we can write Z_i as a polynomial function of the ciphertext, so that $Z_i = p(C_i)$ for some low-degree polynomial $p(x) = a_d x^d + \ldots + a_1 x + a_0$ with $d = \deg p$. Then we can conclude that

$$0 = \sum_i Z_i = \sum_i p(C_i) = \sum_i \sum_{j=0}^{d} a_j C_i^j = \sum_{j=0}^{d} \tau_j \cdot a_j \qquad \text{where } \tau_j = \textstyle\sum_i C_i^j. \quad (6)$$

Note that the τ_j's are known, since the ciphertexts are. Treating the coefficients a_j as formal unknowns, we thus see that Eqn. 6 gives us a single linear relation on the $d+1$ variables $a_0, \ldots, a_d$.

If we repeat the above experiment $d+2$ times, obtaining $d+2$ sets of texts following the integral, we will have $d+2$ linear equations in $d+1$ unknowns. Applying Gaussian elimination, we will find a linear relationship that the ciphertexts must obey when this block cipher is used.

In other words, this allows a distinguishing attack on the underlying block cipher. When the first half of the cipher can be covered by an integral containing 2^s plaintexts, and when the second half can be expressed as a polynomial of degree d, the complexity of the attack will be approximately $d \cdot 2^s$ chosen texts and $d^2 \cdot 2^s + d^3$ work. It is an open question whether these techniques may be effectively extended to apply where we have a probabilistic polynomial relation [14] or rational polynomial relation [13] for the last half of the cipher.

Although we do not know of any concrete examples where this combination yields improved attacks, we conjecture that the opportunity to combine attack techniques in this way may be of interest.

8 Related work

The attack techniques we exploit here were first introduced in [5], but under a different name: these techniques were previously described as “the Square attack”, instead of “integrals.” The name “integrals” has since been proposed independently by both Knudsen [17] and Yu, Zhang, and Xiao [12] to describe this general class of attacks. Also, in [6] the attack was described in terms of “lambda-sets” and applied also to reduced-round versions of the ciphers SHARK [27] and SAFER K [23].

Since their introduction, integrals have been used to cryptanalyse reduced-round versions of Square [5], SAFER K [18], SAFER+ [12], Crypton [8], Rijndael [9], Twofish [22], Hierocrypt [1], IDEA [25], and Camellia [10]. We have shown here additional examples of applications of integrals. Thus, this class of techniques seems to be of broad interest.

Recently Biryukov and Shamir applied a variant of integral cryptanalysis to an SP-network with secret S-boxes and secret linear transformations [4]. They called their technique the *multi-set* attack, where one distinguishes between whether all values in a multi-set are equal, are all different, all occur an even number of times, and where the exclusive-or sum of all values is zero. Thus, there is some resemblence to our definition of integrals and higher-order integrals.

9 Conclusions

In this paper we studied integral cryptanalysis, an attack which applies particularly well to block ciphers that use bijective components. The basic integral attack was introduced some years ago, but without a specific name attached to it. We argued that integral cryptanalysis is the obvious name for the attacks. A powerful extension, the higher-order integral, was given. These new attacks were applied to a range of ciphers. Also, a possible combination of integral cryptanalysis and the interpolation attacks was outlined. We believe that attacks based on higher-order integrals will find many applications in the future.

Acknowledgements

We thank Ulrich Kühn for many helpful comments.

References

1. P. Barreto, V. Rijmen, J. Nakahara Jr., B. Preneel, J. Vandewalle, and H.Y. Kim. "Improved SQUARE attacks against reduced-round HIEROCRYPT". *Fast Software Encryption 2001*, Springer-Verlag, to appear.
2. E. Biham, A. Biryukov, A. Shamir, "Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials," In J. Stern, editor, *Advances in Cryptology: EUROCRYPT'99, LNCS 1592*, pp. 12–23. Springer Verlag, 1999.
3. E. Biham, A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.
4. A. Biryukov, A. Shamir, "Structural Cryptanalysis of SASAS, " *Advances in Cryptology - EUROCRYPT 2001*, LNCS 2045, Springer-Verlag, pp. 394–405, 2001.
5. J. Daemen, L. Knudsen, and V. Rijmen. The block cipher Square. In E. Biham, editor, *Fast Software Encryption, Fourth International Workshop, Haifa, Israel, January 1997, LNCS 1267*, pages 149–165. Springer Verlag, 1997.
6. J. Daemen, L.R. Knudsen, and V. Rijmen, "Linear Frameworks for Block Ciphers," Designs, Codes and Cryptography, Volume 22, No 1, 2001, pp. 65-87.
7. J. Daemen, V. Rijmen, "AES Proposal: Rijndael," *AES Round 1 Technical Evaluation CD-1: Documentation*, National Institute of Standards and Technology, Aug 1998.
8. C. D'Halluin, G. Bijnens, V. Rijmen, and B. Preneel. Attack on Six Rounds of Crypton. In L. Knudsen, editor, *Fast Software Encryption, Sixth International Workshop, Rome, Italy, March 1999, LNCS 1636*, pages 46–59. Springer Verlag, 1999.
9. N. Ferguson, J. Kelsey, B. Schneier, M. Stay, D. Wagner, and D. Whiting. Improved cryptanalysis of Rijndael. In B. Schneier, editor, *Fast Software Encryption, 7th International Workshop, FSE 2000, New York, USA, April 2000, LNCS 1978*, pages 213–230. Springer Verlag, 2001.
10. Y. He, S. Qing, "Square Attack on Reduced Camellia Cipher", *ICICS 2001*, LNCS 2229, Springer-Verlag.
11. I.N. Herstein, *Topics in Algebra*, 2nd ed., John Wiley & Sons, 1975.
12. Y. Hu, Y. Zhang, and G. Xiao, "Integral cryptanalysis of SAFER+", *Electronics Letters*, vol.35, (no.17), IEE, 19 Aug. 1999, p.1458-1459.

13. T. Jakobsen and L. Knudsen. The interpolation attack on block ciphers. In E. Biham, editor, *Fast Software Encryption, Fourth International Workshop, Haifa, Israel, January 1997, LNCS 1267*, pages 28–40. Springer Verlag, 1997.
14. T. Jakobsen, Cryptanalysis of block ciphers with probabilistic non-linear relations of low degree. In H. Krawczyk, editor, *Advances in Cryptology: CRYPTO'98, LNCS 1462*, pages 212–222. Springer Verlag, 1998.
15. L.R. Knudsen and T. Berson. Truncated differentials of SAFER. In Gollmann D., editor, *Fast Software Encryption, Third International Workshop, Cambridge, UK, February 1996, LNCS 1039*, pages 15–26. Springer Verlag, 1995.
16. L.R. Knudsen. Truncated and higher order differentials. In B. Preneel, editor, *Fast Software Encryption - Second International Workshop, Leuven, Belgium, LNCS 1008*, pages 196–211. Springer Verlag, 1995.
17. L.R. Knudsen, "Block Ciphers: State of the Art". Copies of transparencies for lecture at the International Course on State of the Art and Evolution of Computer Security and Industrial Cryptography, Katholieke Universiteit Leuven, Belgium, June, 1997.
18. L.R. Knudsen, "A Detailed Analysis of SAFER K", *Journal of Cryptology*, vol.3, no.4, Springer-Verlag, 2000, pp.417–436.
19. U. Kühn. Cryptanalysis of reduced-round MISTY. In B. Pfitzmann, editor, *Advances in Cryptology - EUROCRYPT'2001, LNCS 2045*, pages 325–339. Springer Verlag, 2001.
20. U. Kühn, "Improved Cryptanalysis of MISTY1," These proceedings.
21. X. Lai, "Higher Order Derivations and Differential Cryptanalysis," *Communications and Cryptography: Two Sides of One Tapestry*, Kluwer Academic Publishers, 1994, pp. 227–233.
22. S. Lucks, "The Saturation Attack—a Bait for Twofish", *Fast Software Encryption 2001*, Springer-Verlag, to appear.
23. J.L. Massey. SAFER K-64: A byte-oriented block-ciphering algorithm. In R. Anderson, editor, *Fast Software Encryption - Proc. Cambridge Security Workshop, Cambridge, U.K.,* LNCS 809, pages 1–17. Springer Verlag, 1994.
24. M. Matsui. New block encryption algorithm MISTY. In E. Biham, editor, *Fast Software Encryption, Fourth International Workshop, Haifa, Israel, January 1997*, LNCS 1267, pages 54–68. Springer Verlag, 1997.
25. J. Nakahara Jr., P.S.L.M. Barreto, B. Preneel, J. Vandewalle, H.Y. Kim, "SQUARE Attacks Against Reduced-Round PES and IDEA Block Ciphers", IACR Cryptology ePrint Archive, Report 2001/068, 2001.
26. K. Nyberg. Generalized Feistel networks. In Kwangjo Kim and Tsutomu Matsumoto, editors, *Advances in Cryptology - ASIACRYPT'96, LNCS 1163*, pages 91–104. Springer Verlag, 1996.
27. V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, and E. De Win. The cipher SHARK. In Gollmann D., editor, *Fast Software Encryption, Third International Workshop, Cambridge, UK, February 1996, LNCS 1039*, pages 99–112. Springer Verlag, 1996.
28. K. Sakurai and Y. Zheng, "On Non-Pseudorandomness from Block Ciphers with Provable Immunity against Linear Cryptanalysis", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science*, Vol. E80-A, No.1, 1997, pp.19-24.