A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-up Lemma

Carlo Harpes, Gerhard G. Kramer, James L. Massey

Swiss Federal Institute of Technology,
Signal and Info. Proc. Lab., CH-8092 Zürich
email: harpes@isi.ee.ethz.ch

Abstract. Matsui's linear cryptanalysis for iterated block ciphers is generalized by replacing his linear expressions with I/O sums. For a single round, an I/O sum is the XOR of a balanced binary-valued function of the round input and a balanced binary-valued function of the round output. The basic attack is described and conditions for it to be successful are given. A procedure for finding effective I/O sums, i.e., I/O sums yielding successful attacks, is given. A cipher contrived to be secure against linear cryptanalysis but vulnerable to this generalization of linear cryptanalysis is given. Finally, it is argued that the ciphers IDEA and SAFER K-64 are secure against this generalization.
Keywords. Linear cryptanalysis, differential cryptanalysis, piling-up lemma, IDEA, SAFER K-64.

1 Introduction

Linear cryptanalysis, which was introduced by Matsui in [5] to attack DES, is an attack that applies to any iterated block cipher. In this paper, we develop a generalized version of linear cryptanalysis that widens somewhat the class of ciphers for which the attack will be successful and that provides additional insight into Matsui's attack.

In Section 2, we define an I/O sum for one round as the XOR of a balanced binary-valued function of the round input and a balanced binary-valued function of the round output. This generalizes Matsui's "linear expressions". We also introduce key-dependent imbalance and average-key imbalance as measures for the usefulness of an I/O sum.

In Section 3, we adapt Matsui's linear cryptanalysis to the use of I/O sums. We describe a basic attack that exploits a multi-round I/O sum for the entire cipher excluding the last round and tries to find the last-round key. In Section 4, we formulate the hypothesis of wrong-key randomization, which states that using a wrong key in the last round to estimate an I/O sum decreases its key-dependent imbalance. The generalized attack succeeds if it is based on an I/O sum satisfying this hypothesis and if enough plaintext/ciphertext pairs are available.

Section 5 treats the case where the average-key imbalance of an I/O sum is unknown. To handle this case, we introduce a threefold sum as an I/O sum XOR-ed with a binary-valued function of the key and show that the imbalance of the

threefold sum is a lower bound on the average-key imbalance of the parent I/O sum. In practice, finding effective I/O sums is done by finding effective threefold sums whose imbalance is much easier to compute.

In Section 6, we develop a procedure for finding effective "homomorphic" threefold sums. This procedure relies on Matsui's piling-up lemma and applies to ciphers whose round function is a cascade of a keyed group operation and a possibly-keyed bijective function. We argue that ciphers that insert keys by certain modulo operations, such as IDEA and SAFER K-64, are generally resistant to this procedure, and we show that, after a slight modification, the procedure can be applied to DES-like ciphers too.

Section 7 defines QRweak, a mini-cipher vulnerable to the generalization of linear cryptanalysis, but secure against differential and linear cryptanalysis. We also argue that the cipher IDEA is secure against the generalization of linear cryptanalysis by showing that the presented procedure for finding effective homomorphic threefold sums finds no effective threefold sum for one round of either IDEA(8) or IDEA(16). We also show that SAFER K-64 has this desirable property.

Section 8 summarizes the main results.

2 Preliminaries

An *r-round iterated block cipher of block-size n* (Fig. 1) consists of r successive applications of a *keyed round function*, with a different key in each round. The *full key* is $K^{(1..r)} := (K^{(1)}, \ldots, K^{(r)})$, where $K^{(i)}$ is the *round key* applied in the i-th *round* for $i = 1, 2, \ldots, r$. The round keys take on values in a set $\mathcal{K}$, the *round key space*. The plaintext X and ciphertext Y take values in $\mathcal{X}$, the set of binary n-tuples. For each round key k, the keyed round function F_k is a bijection on $\mathcal{X}$. Let $Y^{(i)}$ denote the output n-tuple of the i-th round so that $Y = Y^{(r)}$, and let $Y^{(0)} := X$.

Throughout this paper, capital letters such as X, Y, $Y^{(1)}$, $\tilde{Y}^{(r-1)}$, $K^{(1)}$, etc. will denote random variables and the corresponding lowercase letters will denote specific values of these random variables, e.g., fixed keys. A superscript will specify the round(s) to which a variable is associated, e.g., $Y^{(r-1)}$ is the output of the $(r-1)$-th round, $K^{(1..r-1)}$ is the tuple of round keys from the first to the $(r-1)$-th round, etc.

We always assume that the plaintext and all keys used within the cipher are independent and uniformly random over the appropriate spaces, except when we explicitly fix the keys by specifying, e.g., $K^{(1..r)} = k^{(1..r)}$. This assumption defines the random experiment on which linear cryptanalysis is formalized and for which all probabilities are calculated. A binary-valued function is *balanced* if it takes on the value 0 for exactly half of its possible arguments and the value 1 otherwise.

In [5], Matsui exploits a cipher's weakness that he expresses in terms of "linear expressions". In Matsui's terminology, a linear expression for one round is an "equation" for a certain modulo-two sum of round input bits and round output bits as a sum of round key bits. The expression should be satisfied with

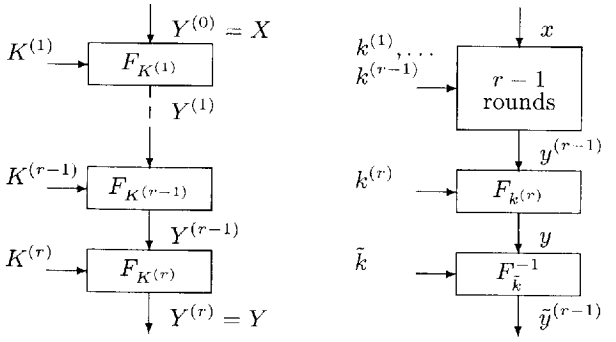

Fig. 1. Structure and notation for an iterated block cipher (left) and notation used in the attack (right).

probability much more (or much less) than 0.5 to be useful. Our generalization of linear cryptanalysis resides in replacing Matsui's linear expressions by the more general notion of I/O sums.

Definition 1. An *I/O sum* $S^{(i)}$ for the i-th round is a modulo-two sum of a balanced binary-valued function f_i of the round input $Y^{(i-1)}$ and a balanced binary-valued function g_i of the round output $Y^{(i)}$, that is,

$$S^{(i)} := f_i(Y^{(i-1)}) \oplus g_i(Y^{(i)}) \ , \tag{1}$$

where $\oplus$ denotes modulo-two addition, i.e., the XOR operation.

The functions f_i and g_i will be called the *input function* and the *output function*, respectively, of the I/O sum $S^{(i)}$.

I/O sums for successive rounds are *linked* if the output function of each round before the last coincides with the input function of the following round (i.e., $f_i = g_{i-1}$). When ρ successive $S^{(i)}$ are linked, their sum,

$$S^{(1..\rho)} := \bigoplus_{i=1}^{\rho} S^{(i)} = g_0(Y^{(0)}) \oplus g_\rho(Y^{(\rho)}) \tag{2}$$

will be called a *multi-round I/O sum.*

As a measure for the "effectiveness" of a linear expression in an attack, Matsui uses the magnitude of the difference between $\frac{1}{2}$ and the probability that the expression is satisfied. We will instead use "imbalances", which are similarly defined but with an extra factor of two so that the imbalance will lie between 0 and 1 inclusive.

Definition 2. The *imbalance* $I(V)$ of a binary-valued random variable V (whose values are the real numbers 0 and 1) is the non-negative real number $|2P[V = 0] - 1|$ or, equivalently, $|E[2V - 1]|$, where $P[V = 0]$ is the probability that V takes on the value 0 and $E[.]$ denotes expectation.

The *key-dependent imbalance* $I(S^{(1..\rho)} \mid k^{(1..\rho)})$ of the I/O sum $S^{(1..\rho)}$ is the imbalance of this sum conditioned on the event that $K^{(1..\rho)} = k^{(1..\rho)}$. The *average-key imbalance* of the I/O sum $S^{(1..\rho)}$ is the expectation of these key-dependent imbalances and will be denoted as $\overline{I}(S^{(1..\rho)})$. An I/O sum is *effective* if it has a large average-key imbalance, and is *guaranteed* if its average-key imbalance is 1, the maximum possible.

As an example, suppose that $S^{(1)} = f(X) \oplus g(Y^{(1)}) = h(K^{(1)})$ where h is a balanced function. Then $S^{(1)}$ has imbalance $I(S^{(1)}) = I(h(K^{(1)})) = 0$. However, because $S^{(1)} = h(k^{(1)})$, a constant, when $K^{(1)} = k^{(1)}$, the key-dependent imbalance of $S^{(1)}$ is 1 for all keys $k^{(1)}$ and hence the average-key imbalance is also 1. Thus $S^{(1)}$ is a guaranteed I/O sum.

3 Attacks by the Generalization of Linear Cryptanalysis

The *basic* attack by the generalization of linear cryptanalysis exploits an effective I/O sum $S^{(1..r-1)} = g_0(X) \oplus g_{r-1}(Y^{(r-1)})$ for the first $r-1$ rounds with the intention of finding the last-round key. It is assumed that the attacker has access to N plaintext/ciphertext pairs (hereafter called *p/c-pairs*) with *uniformly randomly* chosen plaintexts [although experience suggests that *any* N different p/c-pairs will do just as well]. The basic attack proceeds as follows (Fig. 1).

0. Set up a counter $c[\tilde{k}]$ for each possible last-round key $\tilde{k}$ and initialize all counters to 0.
1. Choose a p/c-pair (x, y).
2. For each possible $\tilde{k}$, evaluate $\tilde{y}^{(r-1)} := F_{\tilde{k}}^{-1}(y)$ and, if $g_0(x) \oplus g_{r-1}(\tilde{y}^{(r-1)}) = 0$, increment $c[\tilde{k}]$ by 1.
3. Repeat Step 1 and 2 for all N available p/c-pairs.
4. Output all keys $\tilde{k}$ that maximize $|c[\tilde{k}] - \frac{N}{2}|$ as candidates for the key actually used in the last round.

The quantity $c[\tilde{k}]$ is proportional to an obvious estimate of the key-dependent imbalance of the I/O sum under the assumption that $\tilde{k}$ is the right key. Under suitable statistical assumptions, Step 4 implements the maximum-likelihood decision rule for the last-round key when the counts are considered to be the observation [8].

The basic attack must in practice be speeded up by exploiting "key equivalence". Two keys $k, k' \in \mathcal{K}$ are *equivalent* if $g_{r-1}(F_{k'}^{-1}(y)) = g_{r-1}(F_k^{-1}(y)) \oplus c$ for some c and for all $y \in \mathcal{X}$. The basic attack can never distinguish between equivalent keys. Therefore, we consider in Step 2 only one representative of each *key (equivalence) class*. Just as differential and conventional linear cryptanalysis determine only some portion of the last-round key, the generalization of linear cryptanalysis determines only the (equivalence) class in which the true key lies. The key class containing the actual key used in the last round is the *right class* and its representative is the *right key*. The other key classes are *wrong classes* and their representatives are *wrong keys*. In practice, the number of key classes

must be reasonably small, since the computation in the attack is proportional to that number.

The *success probability* p_{GLC} of the attack is the probability of the event that the output list contains only the right class. The *conditional success probability* $p_{\mathrm{GLC}|k^{(1..r)}}$ is the probability of this event when the key $K^{(1..r)} = k^{(1..r)}$. Matsui considers in [6] an improvement of linear cryptanalysis similar to "list decoding" of error-detecting codes [3]. Applied to our generalization, this improvement consists of trying out all keys in all equivalence classes in order of decreasing apparent imbalance $|c[\tilde{k}] - \frac{N}{2}|$ until the true key is found. The basic attack can also be speeded up (as was done in [6]) by first classifying all p/c-pairs in Step 2 into text classes – each consisting of p/c-pairs that cause the same set of counters to be incremented – and then incrementing the counters once for each text class. Matsui also improved his attack by determining the key to the first and the last round simultaneously [6]. We can use an $(r-2)$-round I/O sum $S^{(2..r-1)}$ instead of $S^{(1..r-1)}$ for a similar improvement of our basic attack.

4 Success of the Generalization of Linear Cryptanalysis

Theorem 3 below states that using enough p/c-pairs in the basic generalization of linear cryptanalysis reveals information on the last-round key provided that the following hypothesis holds.

Hypothesis of wrong-key randomization for an (r-1)-round I/O sum. *Let $S^{(1..r-1)} = g_0(X) \oplus g_{r-1}(Y^{(r-1)})$ be an effective I/O sum for the cipher in Fig. 1. Then, for virtually all possible full keys $k^{(1..r)}$ and for all wrong keys $\tilde{k}$ for the last round, the key-dependent imbalance $I(S^{(1..r-1)} \mid k^{(1..r-1)})$ is substantially reduced if the output of the $(r-1)$-th round is replaced by the estimate $\tilde{Y}^{(r-1)}$ computed from the ciphertext Y and a wrong key $\tilde{k}$ for the last round. That is, for all wrong keys $\tilde{k}$,*

$$\frac{I(\tilde{S}^{(1..r-1)} \mid k^{(1..r)}\tilde{k})}{I(S^{(1..r-1)} \mid k^{(1..r-1)})} << 1 \tag{3}$$

where $\tilde{S}^{(1..r-1)} = g_0(X) \oplus g_{r-1}(\tilde{Y}^{(r-1)})$ and $\tilde{Y}^{(r-1)} = F_{\tilde{k}}^{-1}(Y)$.

$\tilde{S}^{(1..r-1)}$ can be considered as a kind of $(r+1)$-round I/O sum where the $(r+1)$-th round has round function F^{-1} and fixed round key $\tilde{k}$ (Fig. 1, right), but it coincides with either $S^{(1..r-1)}$ or its complement if $\tilde{k}$ is a representative of the right key class (as this implies $g_{r-1}(Y^{(r-1)}) = g_{r-1}(\tilde{Y}^{(r-1)}) \oplus c$). For a good cipher, the key-dependent imbalance of multi-round I/O sums can be expected to decrease with an increasing number of rounds.

Theorem 3. *Suppose that $S^{(1..r-1)}$ is an effective $(r-1)$-round I/O sum for which the hypothesis of wrong-key randomization in the basic attack holds. Then, for virtually all keys, the generalization of linear cryptanalysis with I/O sum $S^{(1..r-1)}$ finds the key class in which the true key of the last round lies as reliably as desired provided that sufficiently many (randomly chosen) p/c-pairs are available.*

By using similar arguments, Matsui showed that, for a fixed key $k^{(1..r)}$, the success probability of linear cryptanalysis is approximately proportional (in our notation) to $(I(S^{(1..r-1)} \mid k^{(1..r)}))^2$ where $S^{(1..r-1)}$ is the considered I/O sum [6, 5]. The crucial point is that the success probability is an increasing function of the key-dependent imbalance of the considered I/O sum, which suggests that this imbalance is a robust measure for the usefulness of such a sum.

5 Random Keys and Threefold Sums

The success probability p_{GLC} of an attack exploiting the I/O sum $S^{(1..r-1)}$ depends on the average-key imbalance $\overline{I}(S^{(1..r-1)})$ in approximately the same manner as $p_{\mathrm{GLC}|k^{(1..r)}}$ depends on $I(S^{(1..r-1)} \mid k^{(1..r)})$. This approximation is virtually exact when the key-dependent imbalances for all keys are virtually equal. We state this as a hypothesis, which is analogous to the hypothesis of stochastic equivalence for differential cryptanalysis [2].

Hypothesis of fixed-key equivalence for an I/O sum. *The key-dependent imbalance of an effective I/O sum $S^{(1..r-1)}$ is virtually independent of the key $k^{(1..r-1)}$; more precisely,*

$$I(\, S^{(1..r-1)} \mid k^{(1..r-1)}) \;\approx\; \overline{I}(S^{(1..r-1)}) \tag{4}$$

is satisfied for virtually all keys $k^{(1..r-1)}$ that can result from the cipher's key scheduling algorithm.

In fact, the average-key imbalance gives us valuable information even without the hypothesis of fixed key equivalence. For example, if $\overline{I}(S^{(1..r-1)}) = 2^{-100}$, we know that at most a fraction 2^{-40} of the keys will give a key-dependent imbalance greater than 2^{-60}. Such an argument allows one to bound the number of "weak keys" for a cipher and suggests that average-key imbalance is a robustly good measure for the usefulness of an I/O sum.

The cryptanalyst needs to find I/O sums that are effective for many (or virtually all) keys. One possibility is to assume that the given hypothesis holds for any I/O sum, fix the key, calculate the key-dependent imbalance by Monte Carlo methods for virtually all possible I/O sums, and then select the most effective ones. We describe below an alternative procedure that requires far less computation. To formulate this procedure requires us to introduce the notion of threefold sums.

Definition 4. A *threefold sum* $T^{(i)}$ for the i-th round is a modulo-two sum of three terms: the first, a balanced binary-valued function f_i of the round input $Y^{(i-1)}$; the second, a balanced binary-valued function g_i of the round output $Y^{(i)}$; and the third, some binary-valued function h_i of the round key $K^{(i)}$; i.e.,

$$T^{(i)} := f_i(Y^{(i-1)}) \oplus g_i(Y^{(i)}) \oplus h_i(K^{(i)}) \;. \tag{5}$$

The function h_i is the *key function* of the threefold sum. Note that the first part of the expression for $T^{(i)}$ is the I/O sum $S^{(i)}$ (cf. (1)). We will call $S^{(i)}$ the *parent* I/O sum for $T^{(i)}$. The imbalance of a threefold sum is calculated under our universal assumption that the arguments of the input function and of the key function are independent and uniformly distributed.

We now analyze the relation between threefold sums and their parent I/O sums. We begin by lower bounding the average-key imbalance of the parent I/O sum $S^{(1..\rho)}$ by the imbalance of the threefold sum $T^{(1..\rho)} = S^{(1..\rho)} \oplus h(K^{(1..\rho)})$ in the manner

$$\begin{aligned} \overline{I}(S^{(1..\rho)}) &= E\left[\left|2P[S^{(1..\rho)}=0 \mid K^{(1..\rho)}]-1\right|\right] \\ &= E\left[\left|2P[T^{(1..\rho)}=0 \mid K^{(1..\rho)}]-1\right|\right] \\ &\geq \left|2E[T^{(1..\rho)}]-1\right| = I(T^{(1..\rho)}) \ , \end{aligned} \tag{6}$$

where we have used Jensen's inequality and the convexity of the absolute-value function. Furthermore, equality holds if and only if $2P[T^{(1..\rho)} = 0 | K^{(1..\rho)} = k^{(1..\rho)}] - 1$ has the same sign for all $k^{(1..\rho)}$. When equality holds, we will call the key function h a *maximizing key function* of $T^{(1..\rho)}$. We thus have proved the following proposition.

Proposition 5. [Threefold sums with maximizing key function] *Let $S^{(1..\rho)}$ be a multi-round I/O sum. Then the function $h_{\max}$ on $\mathcal{K}^\rho$ defined as*

$$h_{\max}(k^{(1..\rho)}) = \begin{cases} 0 & \text{if } P[S^{(1..\rho)} = 0 \mid K^{(1..\rho)} = k^{(1..\rho)})] \geq \frac{1}{2} \\ 1 & \text{otherwise} \end{cases} \tag{7}$$

is a function h which maximizes the imbalance of the multi-round threefold sums $S^{(1..\rho)} \oplus h(K^{(1..\rho)})$, i.e., which upper bounds the imbalance of any other threefold sum with the same parent. Furthermore, this maximum imbalance is the average-key imbalance of the parent I/O sum, i.e.,

$$\overline{I}(S^{(1..\rho)}) \ = \ I(S^{(1..\rho)} \oplus h_{\max}(K^{(1..\rho)})) \ . \tag{8}$$

The example below indicates that the $(r-1)$-round threefold sums used in Matsui's linear cryptanalysis of DES are not likely to have a maximizing key function – thus their imbalances provide only a lower bound on the average-key imbalance of the parent I/O sum. Matsui's approximated success probability is then a pessimistic estimate of the true success probability. In fact, Matsui has noted that his attacks perform better than predicted.

We show in Section 6 how to find the imbalance of threefold sums $S \oplus h(K)$ for a particular family $\mathcal{H}$ of key functions h. Obviously $\overline{I}(S) \geq \max_{h \in \mathcal{H}} I(S \oplus h(K))$, but the right side is often a good approximation to $\overline{I}(S)$. As it is generally infeasible to compute $\overline{I}(S)$ exactly, one has to rely on such an approximation when trying to find effective threefold sums. Section 6 describes such families of key functions for which we are able to compute this approximate imbalance.

Example 1. This example illustrates that if a threefold sum is the sum of threefold sums that are linked, in the sense that their parent I/O sums are linked, and that have maximizing key functions, then this threefold sum can still have a key function that is not maximizing. Consider the cipher in Fig. 2 consisting of a cascade of an MA-box for four input bits ($\mathcal{X} = \{0,1\}^4$) as defined for the cipher IDEA [2], an XOR operation with a four-bit key, and another MA-box.

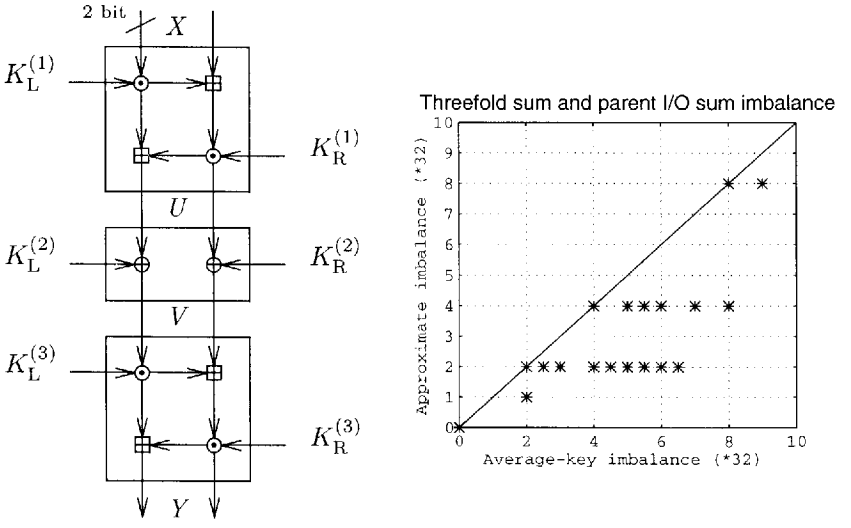

Fig. 2. Cipher using the MA-structure of IDEA(8).

Consider the threefold sum

$$T_{a,b,c} := (a \bullet X) \oplus (c \bullet Y) \oplus (h_{\max,a,b}(K^{(1)}) \oplus (b \bullet K^{(2)}) \oplus h_{\max,b,c}(K^{(3)}))$$

where $h_{\max,a,b}$ and $h_{\max,b,c}$ are the maximizing key functions of

$$T^{(1)}_{\max,a,b} := (a \bullet X) \oplus (b \bullet U) \oplus h_{\max,a,b}(K^{(1)}) \text{ and}$$
$$T^{(3)}_{\max,b,c} := (b \bullet V) \oplus (c \bullet Y) \oplus h_{\max,b,c}(K^{(3)}) \ ,$$

respectively, where $\bullet$ denotes the bitwise scalar product, and where $a, b, c \in \mathcal{X}$. Let $T^{(2)}_{\max,b,b} := (b \bullet U) \oplus (b \bullet V) \oplus (b \bullet K^{(2)})$, so that $T_{a,b,c} = T^{(1)}_{\max,a,b} \oplus T^{(2)}_{\max,b,b} \oplus T^{(3)}_{\max,b,c}$. We show in the next section that $I(T_{a,b,c}) = I(T^{(1)}_{\max,a,b}) \cdot I(T^{(3)}_{\max,b,c})$ as $I(T^{(2)}_{\max,b,b}) = 1$.

In Fig. 2, we compare the approximate imbalance $\max_{b \in \mathcal{X}} I(T_{a,b,c})$ and the average-key imbalance of the parent I/O sum $S_{a,c} := (a \bullet X) \oplus (c \bullet Y)$. For each of the 225 pairs (a, c) for which $a \neq 0$ and $c \neq 0$, we plot one star, which may

overlap with other stars. To compute the average-key imbalances of the I/O sum, we have to find the cipher output for each key and input combination. For such a small cipher, this is still feasible.

We observe that the average-key imbalances of the I/O sum may be strictly larger than the approximate imbalances, even for a pair yielding the greatest approximate imbalance. It follows that the sum of threefold sums each with maximizing key function does not always have a maximizing key function, even if the imbalance of this sum is the largest possible. There are eight threefold sums with the greatest average-key imbalance $9/32$, e.g., the one with $(a, c) = (2, 10)$.[1] If one of these threefold sums is used in an attack, the estimation of the success probability based on the approximate imbalance $8/32$ will be pessimistic. Nonetheless, the highest approximate imbalance is quite close to the true average-key imbalance.

Finally, we analyze one of the most effective I/O sums, namely the one with $(a, c) = (2, 10)$, more closely. The key-dependent imbalances vary between

$$I(S_{2,10}(k^{(1..3)} = (5, 2, t))) = 0 \text{ and } I(S_{2,10}(k^{(1..3)} = (5, 0, t))) = 0.5$$

for $t \in \{0, 1\}^4$. This means that the hypothesis of fixed-key equivalence is not valid.

6 Finding Effective Threefold Sums

6.1 Applicability of Matsui's "Piling-Up Lemma"

In the language of threefold sums, Matsui's piling-up lemma becomes the statement that the imbalance of a sum of threefold sums is the product of their imbalances, i.e.,

$$I\left(\bigoplus_{i=1}^{\rho} T^{(i)}\right) = \prod_{i=1}^{\rho} I(T^{(i)}) \ , \tag{9}$$

provided that these threefold sums are *independent*.

Example 2. Consider a cascade of two "two-bit"-adders – $Y^{(1)} = K^{(1)} \boxplus X$ and $Y^{(2)} = K^{(2)} \boxplus Y^{(1)}$, where $\boxplus$ denotes addition modulo $2^n = 4$ – and the linked threefold sums

$$T^{(1)} = \mathrm{MSB}(X) \oplus \mathrm{MSB}(Y^{(1)}) \oplus \mathrm{MSB}(K^{(1)}) \ ,$$
$$T^{(2)} = \mathrm{MSB}(Y^{(1)}) \oplus \mathrm{MSB}(Y^{(2)}) \oplus \mathrm{MSB}(K^{(2)}) \ ,$$

where the function MSB gives the most significant bit of its argument. It is easy to check that $I(T^{(1)}) = I(T^{(2)}) = \frac{1}{2}$ (the threefold sums are equal to 0 if there is no carry bit, i.e., with probability $\frac{1}{4}$) and yet $I(T^{(1)} \oplus T^{(2)}) = 0 \neq I(T^{(1)}) \cdot I(T^{(2)})$.

[1] In this paper, the usual radix two representation of integers as n-tuples of $\mathcal{X}$ is considered, except sometimes when we consider multiplication, where the all zero n-tuple denotes the integer 2^n.

Thus, the piling-up formula does not hold and hence we can conclude that $T^{(1)}$ and $T^{(2)}$ are *not* independent. We also note that $T^{(1)} \oplus T^{(2)}$ does not have a maximizing key function and that the average-key imbalance of the parent I/O sum is $\frac{1}{2}$, which also does not satisfy the piling-up formula.

The reason that Matsui's piling-up lemma is of interest is that, in actual ciphers, it is infeasible to evaluate a multi-round imbalance directly, as this would involve evaluating the multi-round output for all input and key combinations. One is forced to find imbalances of one-round threefold sums and then use Matsui's piling-up lemma to find the imbalance of their sum. If these one-round threefold sums are linked, we thus get the multi-round threefold sum imbalance, which gives a lower bound on the average-key imbalance of the parent I/O sum. The above example indicates the desirability of conditions guaranteeing the independence of one-round threefold sums, since the piling-up formula (9) applied to dependent threefold sums can suggest misleading results. The following lemma specifies such a condition.

Lemma 6. *For an iterated cipher as in Fig. 1 with independent round keys, let $T^{(i)}$ be a threefold sum for the i-th round. If for each $i = 2, \ldots, \rho$, $T^{(i)}$ is independent of the round input $Y^{(i-1)}$, then the threefold sums $T^{(1)}, \ldots, T^{(\rho)}$ are independent.*

6.2 A Procedure for Finding Effective "Homomorphic" Threefold Sums

The independence of a one-round threefold sum and its input can be assured when a group operation occurs at the beginning of each round. This fact is fundamental for Theorem 8. Hereafter, we denote the left and the right part of a key $K^{(i)}$ by $K_{\mathrm{L}}^{(i)}$ and $K_{\mathrm{R}}^{(i)}$, respectively.

Definition 7. An I/O sum is *homomorphic* if the input and the output functions are homomorphisms for some considered group operation(s). A threefold sum is homomorphic if the parent I/O sum is homomorphic.

For example, a one-round homomorphic threefold sum, independent of its input, for a cipher that inserts the key $K_{\mathrm{L}}^{(i)}$ with the group operation "$*_i$" at the entry of the i-th round, is

$$T^{(i)} := f_i(Y^{(i-1)}) \oplus g_i(Y^{(i)}) \oplus (f_i(K_{\mathrm{L}}^{(i)}) \oplus h_i(K_{\mathrm{R}}^{(i)})) \ , \tag{10}$$

where f_i and g_i are homomorphic binary functions for $*_i$ and $*_{i+1}$, respectively, i.e., for all $U, V \in \mathcal{X}$, $f_i(U *_i V) = f_i(U) \oplus f_i(V)$ and $g_i(U *_{i+1} V) = g_i(U) \oplus g_i(V)$.

Theorem 8. *Consider a cascade of ρ rounds with keyed round functions $F^{(1)}, \ldots F^{(\rho)}$, for which*

$$Y^{(i)} = F_{K^{(i)}}^{(i)}(Y^{(i-1)}) = \phi_i(\, Y^{(i-1)} *_i K_{\mathrm{L}}^{(i)}, K_{\mathrm{R}}^{(i)}\,) \tag{11}$$

where "$*_i$" denotes a group operation in $\mathcal{X}$, $\phi_i(.,k_R^{(i)})$ is a bijection on $\mathcal{X}$ for all $k_R^{(i)}$, $T^{(i)}$ is a homomorphic threefold sum for the i-th round, and $T^{(1)}, \ldots, T^{(\rho)}$ are linked. Then the imbalance of the ρ-round threefold sum $T^{(1..\rho)} := \bigoplus_{i=1}^{\rho} T^{(i)}$ is given by Matsui's piling-up formula (9). This means that for the parent I/O sums,

$$\overline{I}(S^{(1..\rho)}) \geq \prod_{i=1}^{\rho} \overline{I}(S^{(i)}) \geq \prod_{i=1}^{\rho} I(T^{(i)}) \ . \tag{12}$$

It follows that one can find an effective ρ-round threefold sum for a cipher whose round functions have a group operation at the entry (cf. 11) as follows:

1. For $i = 1, \ldots, \rho + 1$, find the set $\mathcal{H}_i$ of all binary functions on $\mathcal{X}$ that are homomorphisms for "$*_i$".
2. For $i = 1, \ldots, \rho$, find the imbalance of all i-th-round homomorphic threefold sums with input function $g_{i-1} \in \mathcal{H}_i$ and output function $g_i \in \mathcal{H}_{i+1}$.
   Discard the threefold sums with small imbalance.
3. Consider each possible list of ρ linked threefold sums containing one threefold sum found in Step 2 for each round.
   Use Theorem 8 to find the imbalance of the ρ-round threefold sum that can be written as the sum of all threefold sums in the same list.
   Find the ρ-round threefold sum with the largest imbalance.

6.3 Discussion of the Given Procedure

The complexity of the above procedure depends mainly on the number of homomorphisms onto $(\{0,1\}, \oplus)$ for the group operations. If "$*_i$" is the bitwise XOR operation in $\mathcal{X}$, the only such homomorphisms are the *linear* functions defined by $l_a(x) = a \bullet x$ for all $x \in \mathcal{X}$, where a is a non-zero n-tuple. An I/O sum (or a threefold sum) whose input and output functions are l_a and l_b, respectively, is called *linear* with *linear-mask* (a, b). If all group operations "$*_i$" are the XOR operation, the given procedure considers only threefold sums whose component functions are linear. Thus for DES and other ciphers using XOR, the given procedure leads to no improvement of Matsui's method for finding effective linear expressions and to no real generalization of his linear cryptanalysis.

For the two groups $(\{0,1\}^n, \odot)$ (multiplication modulo 2^n+1 with $n = 2, 4, 8$ or 16, and 0 representing 2^n) and $(\{0,1\}^n, \boxplus)$ (addition modulo 2^n) of order 2^n used in IDEA [1, 2], there exists only one homomorphism, viz. the quadratic residue function QR for $\odot$ and the parity function (i.e., the least significant bit function LSB) for $\boxplus$. For ciphers using these operations, there are only very few possible linked threefold-sums, so that there is little chance that one of the corresponding threefold sums is effective. Thus the procedure for finding effective homomorphic threefold sums and the generalization of linear cryptanalysis is not very powerful against most ciphers using such operations to insert the key.

It is generally infeasible to analyze the imbalances of all possible threefold sums and even infeasible to find the imbalance of a single $(r-1)$-round threefold sum if one cannot deduce it from the imbalances of smaller sections such as rounds or S-boxes by using Matsui's piling-up lemma. The only threefold sums we know to which Matsui's piling-up lemma applies are homomorphic. We are aware of no practical alternative for finding imbalances. The procedure given in this section considers promising candidates for the most effective threefold sum, but it never guarantees that the threefold sum found is the most effective possible.

Example 3. To show that such a guarantee does not exist, we consider the 3-bit round function F defined by $Y = F_K(X) = \phi(X \boxplus K)$ where the function table of ϕ is $\underline{\phi} := (0,1,3,5,2,4,7,6)$. The only homomorphic function l for $\boxplus$ is given by $\underline{l} = (0,1,0,1,0,1,0,1)$. Since $\overline{I}(l(X) \oplus l(Y)) = 0$, but $\overline{I}(f(X) \oplus l(Y)) = \frac{1}{4}$ for $\underline{f} := (1,1,1,1,0,0,0,0)$, the threefold sum with input function f has higher imbalance than the only homomorphic threefold sum.

6.4 Application to DES

A procedure for finding effective homomorphic threefold sums for DES has been implemented in [7]. It is similar to our procedure, but it requires more ingenuity to link threefold sums efficiently as there exist many guaranteed one-round threefold sums. The following example illustrates how one-round threefold sums that are independent of their input are constructed. By Lemma 6, this guarantees that Matsui's piling-up lemma is applicable when we cascade them.

Example 4. Let U_i denotes the i-th bit of a random variable U, where we number the bits from left to right starting with 1. This differs from Matsui's numbering (right to left starting with 0). For example, what we call the 2nd input bit to an S-box, Matsui calls the 4-th input bit; our 3rd plaintext bit X_3 is his bit $P_{\mathrm{H}}[29]$ and Y_{64} corresponds in his notation to $C_{\mathrm{L}}[0]$.

Let U denote the 6-bit input to the fifth S-box S5, and $V := S5(U)$ the 4-bit output. The threefold sum $U_2 \oplus V_1 \oplus V_2 \oplus V_3 \oplus V_4$ has imbalance $\frac{5}{8}$. By considering the permutation and the expansion in DES, one can find relations that enable us to transform the threefold sum for S5 into the threefold sum

$$T^{(1)} = (X_3^{(1)} \oplus X_8^{(1)} \oplus X_{14}^{(1)} \oplus X_{25}^{(1)} \oplus X_{49}^{(1)}) \oplus (Y_{35}^{(1)} \oplus Y_{40}^{(1)} \oplus Y_{46}^{(1)} \oplus Y_{57}^{(1)}) \oplus K_{26}^{(1)},$$

which has the same imbalance $\frac{5}{8}$ and is independent of the input $X^{(1)}$. Similarly,

$$T^{(3)} = (X_3^{(3)} \oplus X_8^{(3)} \oplus X_{14}^{(3)} \oplus X_{25}^{(3)}) \oplus (Y_{17}^{(3)} \oplus Y_{35}^{(3)} \oplus Y_{40}^{(3)} \oplus Y_{46}^{(3)} \oplus Y_{57}^{(3)}) \oplus K_{26}^{(3)} \ .$$

Since the I/O sum $S^{(2)}$ linked to both $T^{(1)}$ and $T^{(3)}$ is guaranteed, $T^{(1..3)}$ (with $T^{(2)} = S^{(2)}$) has imbalance $I(T^{(1)}) \cdot I(T^{(3)}) = \frac{25}{64}$, which is quite effective.

7 Some Examples

7.1 The QRweak Cipher

We now contrive a cipher, QRweak, to be weak against our generalization of linear cryptanalysis, but secure against linear and differential cryptanalysis. QRweak is a four round iterated block cipher of block-size eight (Fig. 1 with $r = 4$, $n = 8$) whose round function is defined as $F_k(x) = \phi(x \odot k)$, where $\odot$ denotes multiplication modulo 257 and where the function ϕ changes the bit order of the argument in the manner $t_1t_2t_3t_4t_5t_6t_7t_8 \mapsto t_6t_4t_8t_3t_1t_5t_2t_7$ and then XORs the result with the integer 34. The function ϕ of the last round can be omitted. Our aim is to find the key of the last round, given that all p/c-pairs are known. The only homomorphic one-round threefold sum that is independent of the input is $\mathrm{QR}(X) \oplus \mathrm{QR}(Y) \oplus \mathrm{QR}(K)$ and has imbalance $I^{\mathrm{QR}} = \frac{21}{64}$, where QR is the quadratic residues modulo $2^8 + 1$ function. The parent I/O sum of the "two and a half"-round threefold sum

$$\mathrm{QR}(X) \oplus \mathrm{QR}(Y^{(2)} \odot K^{(3)}) \oplus \mathrm{QR}(K^{(1)}) \oplus \mathrm{QR}(K^{(2)}) \oplus \mathrm{QR}(K^{(3)})$$

with imbalance $(\frac{21}{64})^2 = 10.77\%$ is used in our attack. The success probability is $p_{\mathrm{GLC}} \approx 5.5\%$, whereas linear and differential cryptanalysis as well as random key guessing yield a success probability of only about 0.39%.

7.2 Cryptanalysis of IDEA

We now apply the procedure for finding effective homomorphic threefold sums to the cipher IDEA [1], earlier called IPES [2]. The round function is a function on 64-bit words, consisting of a group operation denoted by $\otimes$, a keyed involution In and a permutation P_I. Each 64-bit word X can be considered as a concatenation of four 16-bit words $X1, X2, X3, X4$ and denoted as a 4-tuple. The group operation is defined as $X \otimes K := (X1 \odot K1,\ X2 \boxplus K2,\ X3 \boxplus K3,\ X4 \odot K4)$, where $\odot$ denotes multiplication modulo $2^{16} + 1$ with 0 representing 2^{16}, and $\boxplus$ addition modulo 2^{16}. As there exists only one non-constant homomorphism for $\boxplus$ and only one for $\odot$, there exist $2^4 - 1$ homomorphisms for $\otimes$, namely the functions

$$f_i(X) = (i1 \cdot \mathrm{QR}(X1)) \oplus (i2 \cdot \mathrm{LSB}(X2)) \oplus (i3 \cdot \mathrm{LSB}(X3)) \oplus (i4 \cdot \mathrm{QR}(X4)) \quad (13)$$

for all binary four-tuples $i = i1\,i2\,i3\,i4$ different from 0000, where QR is the quadratic-residue modulo $2^{16} + 1$ function.

A homomorphic I/O sum for IDEA can be characterized by the *IDEA-mask* (a, b) where the non-zero 4-tuple a is the mask of the input function and the non-zero 4-tuple b the mask of the output function.

We try to find effective homomorphic one-round I/O sums. For some of the 225 IDEA-masks, e.g., $(1110, 0100)$, we can show that the average-key imbalance, and thus all key-dependent imbalances, are zero. For other IDEA-masks, it is computationally infeasible to evaluate the key-dependent imbalances exactly. For

the mini-cipher IDEA(8), the average-key imbalance of all one-round homomorphic I/O sums are zero. For IDEA(16), the one-round I/O sums with IDEA-masks $(1111, 1011)$, $(1101, 1111)$, $(1011, 1001)$, and $(1001, 1101)$ have average-key imbalance 0.002441, the four with $(1111, 1001)$, $(1001, 1111)$, $(1101, 1101)$, and $(1011, 1011)$ have average-key imbalance 0.00122, and all other I/O sum average-key imbalances are zero. Moreover, the number of p/c-pairs that must be analyzed in the generalization of linear cryptanalysis is about the square of the key-dependent imbalance and is here far larger than the total number of p/c-pairs. We conclude that the procedure for finding effective homomorphic threefold sums does not find any effective threefold sum for IDEA(8) and IDEA(16). Furthermore, the maximum key-dependent homomorphic I/O sum imbalance is only 0.00586. As this is only slightly larger than the maximum I/O sum average-key imbalance, there are no weak keys for the MA-box with respect to our attack. These conclusions doubtlessly hold true for (full-sized) IDEA as well. Thus IDEA seems secure against the generalization of linear cryptanalysis.

7.3 Cryptanalysis of SAFER K-64

SAFER K-64 is an iterated block-cipher, presented by Massey in [4]. The round function of SAFER K-64 consists of two half-rounds, each consisting of a keyed group operation and an unkeyed bijection either consisting of exponential and logarithm functions modulo 257 or a "Pseudo-Hadamard Transform". We have been able to prove that the procedure for finding effective homomorphic threefold sums for "one and a half" or more rounds of SAFER K-64 does not find a homomorphic threefold sum with non-zero imbalance. We conclude that SAFER K-64 is secure against the procedure for finding effective homomorphic threefold sums.

8 Conclusion

We have defined a generalization of linear cryptanalysis of iterated block ciphers and focused on its basic attack, which exploits an effective $(r-1)$-round I/O sum to find information about the key of the last round. We have given sufficient conditions for a successful basic attack. These results can be extended to non-basic attacks in a manner similar to Matsui's improvements on basic linear cryptanalysis [6].

We have given a careful analysis of the applicability of Matsui's piling-up lemma. For the family of ciphers that insert keys by group operations, we have developed a procedure for finding some (arguably the best, but not necessarily all) effective multi-round threefold sums. This procedure requires finding homomorphisms for the used group operations. For ciphers using XOR (such as DES), the procedure finds only linear threefold sums, which are the same as Matsui's linear expressions. For ciphers using modular addition and multiplication with large moduli (such as IDEA), the choice of homomorphic sums is

severely limited so that such ciphers tend to be immune to our generalization of linear cryptanalysis.

Finally, we argued that IDEA is secure against the generalization of linear cryptanalysis by showing that the presented procedure for finding effective homomorphic threefold sums finds no effective threefold sum for IDEA(8) or for IDEA(16). Similarly, the procedure for finding effective homomorphic threefold sums finds no effective threefold sum for "one and a half" (or more) rounds of SAFER K-64.

9 Acknowledgments

It is a pleasure to thank Richard De Moliner, Thomas Jakobsen, Kenneth Paterson, and Christian Waldvogel for helpful discussions. Thanks also to Patrick Berny, Steve Perkins, and Tobias Zürcher for their enthusiastic assistance in the cryptanalysis of IDEA and SAFER K-64.

References

1. X. Lai, *On the Design and Security of Block Ciphers*, vol. 1 of *ETH Series in Information Processing*. Hartung-Gorre Verlag Konstanz, J. L. Massey ed., 1992. ISBN 3-89191-573-X.
2. X. Lai, J. L. Massey, and S. Murphy, "Markov ciphers and differential cryptanalysis," in *Advances in Cryptology – Eurocrypt'91*, LNCS 574, pp. 17–38, Springer, 1991.
3. S. K. Langford and M. E. Hellman, "Differential-linear cryptanalysis," in *Advances in Cryptology – Crypto'94*, LNCS 839, pp. 17–25, Springer, 1994.
4. J. L. Massey, "SAFER K-64: A byte-oriented block-ciphering algorithm," in *Fast Software Encryption* (R. Anderson, ed.), LNCS 809, pp. 1–17, Springer, Dec. 1993.
5. M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology – Eurocrypt'93*, LNCS 765, pp. 386–397, Springer, 1993.
6. M. Matsui, "The first experimental cryptanalysis of the data encryption standard," in *Advances in Cryptology – Crypto'94*, LNCS 839, pp. 1–11, Springer, 1994.
7. M. Matsui, "On correlation between the order of S-boxes and the strength of DES," in *Advances in Cryptology – Eurocrypt'94*, 1994.
8. S. Murphy, F. Piper, M. Walker, and P. Wild, "Likelihood estimation for block cipher keys." submitted for publication, 1994.