# Partitioning Cryptanalysis

Carlo Harpes, James L. Massey

ETH Zürich, Signal and Info. Proc. Lab., CH-8092 Zürich
CETREL S.C., L-2956 Luxemburg
email: harpes@cetrel.lu, massey@isi.ee.ethz.ch

**Abstract.** Matsui's linear cryptanalysis for iterated block ciphers is generalized to an attack called partitioning cryptanalysis. This attack exploits a weakness that can be described by an effective partition-pair, i.e., a partition of the plaintext set and a partition of the next-to-last-round output set such that, for every key, the next-to-last-round outputs are non-uniformly distributed over the blocks of the second partition when the plaintexts are chosen uniformly at random from a particular block of the first partition. The last-round attack by partitioning cryptanalysis is formalized and requirements for it to be successful are stated. The success probability is approximated and a procedure for finding effective partition-pairs is formulated. The usefulness of partitioning cryptanalysis is demonstrated by applying it successfully to six rounds of the DES.

*Keywords.* Iterated block ciphers, linear cryptanalysis, partitioning cryptanalysis, DES.

## 1 Introduction

In cryptography, frequent use is made of iterated block ciphers in which a keyed function, called the round function, is iterated $r$ times. Linear cryptanalysis, introduced by Matsui in [Mat94b, Mat94a] is a known-plaintext attack that requires the existence of "unbalanced linear expressions". In [HKM95], linear cryptanalysis was generalized by replacing linear expressions with "input/output (I/O) sums". In [Har96, Har94], an even more general attack called *partitioning cryptanalysis* was introduced. This attack is based on the same principle as the statistical attacks independently developed in [MPWW94] and [Vau96]. Similarly to linear and differential cryptanalysis [BS93], partitioning cryptanalysis can be used to evaluate the strength of iterated block ciphers or to detect the existence of backdoors in such ciphers. This paper is intended to provide a thorough treatment of partitioning cryptanalysis and, as a side benefit, to give additional insight into linear cryptanalysis.

In a *last-round attack*, many plaintext/ciphertext-pairs, hereafter called p/c-pairs, are considered. For every considered ciphertext, one guesses the next-to-last-round output by decrypting the last-round with a guessed key. Then, one computes an *empirical decision metric* for this guessed key, which is an estimate of the expectation of some function of some random variable that depends on the plaintext and the guessed next-to-last round output. One repeats this

computation for all last-round key guesses and chooses the key with largest empirical decision metric as the "cryptanalyst's guess" for the actual last-round key.

In the last-round attack by the generalization of linear cryptanalysis, the empirical decision metric is the sample-mean estimate of the "imbalance" of an "I/O sum". The *imbalance* of a binary random variable $V$ is defined to be $I(V) := |2P[V = 0] - 1|$, where $P[V = 0]$ denotes the probability that $V$ is 0. An *I/O sum* is a modulo-two sum of a balanced binary-valued function of the plaintext random variable and a balanced binary-valued function of the guessed next-to-last-round output random variable.

In partitioning cryptanalysis, only p/c-pairs whose plaintexts lie in some fixed block of a partition of the plaintext set, called the *input partition*, are considered. Let $J(\tilde{k})$ be the random variable specifying the block of some chosen *output partition* containing the guessed next-to-last round output, where $\tilde{k}$ is the guessed key used to decrypt the last round. The decision metric is an estimate of the "imbalance" of $J(\tilde{k})$, where an *imbalance* of an $m$-ary random variable $V$ is a measure for how non-uniformly distributed $V$ is. The weakness exploited in partitioning cryptanalysis is thus described by a *partition-pair*, i.e., a pair consisting of an input partition and an output partition, and we will introduce an *imbalance* to measure the effectiveness of a partition-pair in partitioning cryptanalysis. The success of partitioning cryptanalysis relies on the fact that $J(\tilde{k})$ is less balanced when $\tilde{k}$ is the true last-round key than when $\tilde{k}$ is a wrong guess.

In Section 2, we introduce some preliminaries. The last-round attack by partitioning cryptanalysis is developed in Section 3. In Section 4, we give conditions for a successful attack. In Section 5, we consider ciphers in which a part of the round key is inserted by means of a group operation at the inputs to the rounds and we define coset-partitions as partitions whose elements are the cosets of some subgroup with respect to this group operation. To apply partitioning cryptanalysis, there must exist a sufficiently effective partition-pair and the cryptanalyst must have a practical method to find it; in Section 6, we discuss such a method. In Section 7, we apply partitioning cryptanalysis successfully to 6-round DES. We close in Section 8 with a summary of the main results.

In Appendix A, we formulate *combined partitioning cryptanalysis* as an attack that combines several attacks by partitioning cryptanalysis, which attacks exploit the same partition-pair but use p/c-pairs with plaintexts from different blocks of the plaintext partition. In Appendix B, we approximate the success probability of partitioning cryptanalysis. In Appendix C, we provide some details of the partitioning cryptanalysis of 6-round DES.

## 2 Preliminaries

In this section, $Y$ denotes the output of some keyed function $\phi$ whose input is $X$ and whose key is $Z$, i.e., $Y = \phi_Z(X)$. It may be that $\phi$ is the round function of a cipher or the composition of several round functions. It may also be that $\phi$

is unkeyed and not invertible, as when $\phi$ is the function realized by an S-box of DES.

A *partition* of a set $\mathcal{S}$ is a finite set whose elements are pairwise-disjoint non-empty subsets of $\mathcal{S}$ whose union is $\mathcal{S}$. These subsets are called the *blocks* of the partition.

**Definition 1.** Let $\mathcal{F} = \{\mathcal{F}_0, \mathcal{F}_1, \ldots, \mathcal{F}_{l-1}\}$ and $\mathcal{G} = \{\mathcal{G}_0, \mathcal{G}_1, \ldots, \mathcal{G}_{m-1}\}$ be partitions of the input set and the output set, respectively, of a keyed function $\phi_Z$. The pair $(\mathcal{F}, \mathcal{G})$ is a *partition-pair* for $\phi$ if all blocks of $\mathcal{F}$ contain the same number (at least two) of elements, as also do all blocks of $\mathcal{G}$, and if both $l$ and $m$ are at least two.

The blocks of the *input partition* $\mathcal{F}$ will be called *input blocks* and the blocks of the *output partition* $\mathcal{G}$ will be called *output blocks*. The function from the input set of $\phi$ onto $\{0, 1, \ldots, l-1\}$ that maps an element $x$ to the index $i$ of the block $\mathcal{F}_i$ containing $x$ will be called the *partitioning function* of $\mathcal{F}$ and denoted by $f$. Similarly, $g$ will denote the partitioning function of $\mathcal{G}$. Note that $f$ and $g$ are always balanced functions, i.e., functions that take on each of their possible values for the same number of arguments.

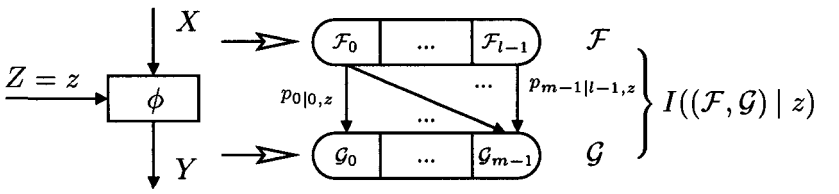



**Fig. 1.** Representation of a partition-pair $(\mathcal{F}, \mathcal{G})$ for $\phi$ given the key $z$.

We use capital letters $X$, $Y$, $Z$, etc., to denote random variables and the corresponding lowercase letters $x$, $y$, $z$, etc., to denote specific values of these random variables. The experiment on which partitioning cryptanalysis relies is the random experiment in which the plaintext and all round keys are chosen independently and uniformly at random over the appropriate sets. Note that, because all blocks of $\mathcal{F}$ have the same size, $f(X)$ is uniformly distributed.

A function of an $m$-ary random variable, taking on real values between 0 and 1, inclusive, and measuring how non-uniformly the random variable is distributed, will be called an *imbalance*. The imbalance of the random variable $V$ will be denoted $I(V)$. We will consider two imbalance measures, namely, the *peak imbalance*

$$I_{\mathrm{p}}(V) \quad := \quad \frac{m}{m-1}\left(\max_{0 \le i < m} P[V=i] - \frac{1}{m}\right)$$

and the *squared Euclidean imbalance*

$$I_2^2(V) := \frac{m}{m-1}\sum_{i=0}^{m-1}\left(P[V=i]-\frac{1}{m}\right)^2 = \frac{m}{m-1}\sum_{i=0}^{m-1}(P[V=i])^2 - \frac{1}{m-1}.$$

The usefulness of a partition-pair for partitioning cryptanalysis will be characterized by a partition-pair imbalance, which also lies between 0 and 1, inclusive.

**Definition 2.** Let $(\mathcal{F},\mathcal{G})$ be a partition-pair for the function with input $X$ and output $Y$ and let $I(.)$ be an imbalance measure for $m$-ary random variables where $m = |\mathcal{G}|$. Let $I(g(Y) \mid f(X)=i)$ denote the imbalance of the random variable $g(Y)$ when conditioned on the event that $f(X) = i$. The *imbalance* $I((\mathcal{F},\mathcal{G}))$ *of the partition-pair* $(\mathcal{F},\mathcal{G})$ is the quantity

$$I((\mathcal{F},\mathcal{G})) := \frac{1}{l}\sum_{i=0}^{l-1} I(g(Y) \mid f(X)=i) \ ,$$

where $l = |\mathcal{F}|$ and where $f$ and $g$ are the partitioning functions of $\mathcal{F}$ and $\mathcal{G}$, respectively.

The notion of key-dependent imbalance is of special importance. Consider the keyed function $\phi_Z$ with key $Z$ taken from a set $\mathcal{Z}$. Let $I(g(Y) \mid f(X)=i,\ Z=z)$ denote the imbalance of the $m$-ary random variable $g(Y)$ when conditioned on the joint event that $f(X) = i$ and $Z = z$. We will call this quantity the *key-dependent input-block-dependent imbalance* of the partition-pair $(\mathcal{F},\mathcal{G})$ for $\phi$. The *key-dependent imbalance* of the partition-pair $(\mathcal{F},\mathcal{G})$ given the key $z$ is the quantity

$$I((\mathcal{F},\mathcal{G})|z) := \frac{1}{l}\sum_{i=0}^{l-1} I(g(Y) \mid f(X)=i,\ Z=z) \ .$$

The *average-key imbalance* of $(\mathcal{F},\mathcal{G})$ is the quantity

$$\overline{I}((\mathcal{F},\mathcal{G})) := \frac{1}{|\mathcal{Z}|}\sum_{z\in\mathcal{Z}} I((\mathcal{F},\mathcal{G}) \mid z) = \frac{1}{l}\sum_{i=0}^{l-1}\overline{I}(g(Y) \mid f(X)=i) \ ,$$

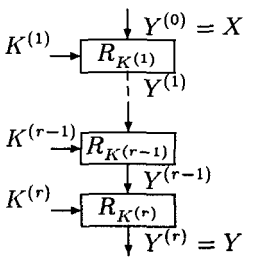
where $\overline{I}(g(Y) \mid f(X)=i)$ denotes the *average-key input-block-dependent imbalance* of $(\mathcal{F},\mathcal{G})$ for the input block $\mathcal{F}_i$.

The imbalance $\overline{I}((\mathcal{F},\mathcal{G}))$ of the partition-pair $(\mathcal{F},\mathcal{G})$ can be calculated from the *key-dependent transition probabilities* $p_{j|i,z}$ for $0 \le i < l$, $0 \le j < m$, and $z$ in $\mathcal{Z}$, where $p_{j|i,z}$ is the conditional probability that the output $Y = \phi_Z(X)$ lies in the output block $\mathcal{G}_j$ given that the input $X$ is chosen uniformly at random in the input block $\mathcal{F}_i$ and that $Z = z$ (cf. Fig. 1).

The partition-pair $(\mathcal{F},\mathcal{G})$ will be said to have *guaranteed transitions* if its average-key imbalance is 1. Guaranteed transitions mean that, for each key, the block of $\mathcal{G}$ in which the output lies is uniquely determined by the key and the block of $\mathcal{F}$ in which the input lies, i.e., *the key and the input block uniquely determine*

*the output block.* The partition-pair is *effective* if its average-key imbalance is substantially greater than zero. This means that the output block is determined with substantially large probability by the key and by the input block.

In the following, we apply partitioning cryptanalysis to *iterated block ciphers* as defined in Fig. 2.




$X$ is the *plaintext*, $Y$ is the *ciphertext*, $K^{(1)}, \ldots, K^{(r)}$ are the round keys, $K^{(1..r)} := (K^{(1)}, \ldots, K^{(r)})$ is the *full key*, and $R$ is the *round function*. The round keys take values in a set $\mathcal{K}$, the *round key set*. $X$ and $Y$ take values in $\mathbb{B}^n$, the set of binary $n$-tuples. For each value $k$ of the round key, the keyed round function $R_k$ is an invertible function on $\mathbb{B}^n$. Let $Y^{(i)}$ denote the output $n$-tuple of the $i$-th round so that $Y = Y^{(r)}$ and let $Y^{(0)} = X$.

**Fig. 2.** Structure and notation for an $r$-round iterated block cipher.

## 3 Last-Round Attack by Partitioning Cryptanalysis

In the last-round attack by partitioning cryptanalysis, we consider a partition-pair $(\mathcal{F}, \mathcal{G})$ for the keyed function consisting of the first $r-1$ rounds of a cipher. Such a partition-pair will be called an $(r-1)$-*round partition-pair.* $\mathcal{F}$ and $\mathcal{G}$ are partitions of $\mathbb{B}^n$ so that the numbers $m$ and $l$ of blocks in these partitions must both be powers of 2. Typically, $m$ will be 2, 4, 8, or 16, and $l \geq m$. For the last-round attack, $Z = K^{(1..r-1)}$ and this key lies in the set $\mathcal{K}^{r-1}$. Let $\mathcal{F}_i$ be the input block used in the attack and suppose that $N$ p/c-pairs with plaintexts in $\mathcal{F}_i$ are known. The attack proceeds as follows.

0. For each $\tilde{k}$ in the set $\tilde{\mathcal{K}}$ of possible last-round keys, set up $m$ counters with one counter $c[\tilde{k}, j]$ for each $j$, $0 \leq j < m$, and initialize all counters to 0.
1. Consider a known p/c-pair $(x, y)$ with plaintext $x$ in $\mathcal{F}_i$.
2. For each $\tilde{k}$ in $\tilde{\mathcal{K}}$, evaluate $\tilde{y}^{(r-1)} := R_{\tilde{k}}^{-1}(y)$ and increment the counter $c[\tilde{k}, g(\tilde{y}^{(r-1)})]$ of the output block in which $\tilde{y}^{(r-1)}$ lies by 1.
3. Repeat Steps 1 and 2 for all $N$ known p/c-pairs $(x, y)$ with $x$ in $\mathcal{F}_i$.
4. Output the key(s) $\tilde{k}$ maximizing $\hat{\mu}(\tilde{k}) = I\left(\frac{c[\tilde{k},0]}{N}, \frac{c[\tilde{k},1]}{N}, \ldots, \frac{c[\tilde{k},m-1]}{N}\right)$ (which, with slight abuse of notation, denotes the imbalance of the random variable whose probability distribution is shown as the argument) as the candidate(s) for the actual key in the last round.

Note that $I(.)$ can be either the peak imbalance or the Euclidean imbalance. The quantity $\hat{\mu}(\tilde{k})$ is an empirical estimate of the decision metric

$$\mu(\tilde{k}) \quad = \quad I(\, g(R_{\tilde{K}}^{-1}(Y)) \mid f(X)=i,\ K^{(1..r)}\tilde{K}=k^{(1..r)}\tilde{k}\,) \ ,$$

which is the key-dependent input-block dependent imbalance of the partition-pair $(\mathcal{F},\mathcal{G})$ for the keyed function whose input is $X$, whose key is the concatenation of $K^{(1\ r)}$ and $\tilde{K}$, and whose output is $R_{\tilde{K}}^{-1}(Y)$.

The last-round attack must in practice be speeded up by exploiting "key equivalence". Two last-round keys $k$ and $k'$ are *equivalent* if there is a bijection $\psi$ of $\{0, 1, \ldots, m-1\}$ such that $g(R_k^{-1}(y)) = \psi(g(R_{k'}^{-1}(y)))$ for all $y$ in $\mathbb{B}^n$. Keys belonging to the same *key equivalence class* produce counter lists $(c[k,0], c[k,1], \ldots, c[k,m-1])$ that differ only by a permutation and hence yield the same empirical decision metric so that they are indistinguishable by the attack. Therefore, we need to consider in Step 2 only one representative of each key (equivalence) class. We will write $\tilde{\mathcal{K}}$ to denote a set containing exactly one representative $\tilde{k}$ of each key class. Partitioning cryptanalysis determines only the class in which the true last-round key $k^{(r)}$ lies. This class is called the *right class* and its representative is the *right key* $\tilde{k}_{\mathrm{r}}$. The other key classes are *wrong classes* and their representatives are *wrong keys* $\tilde{k}_{\mathrm{w}}$ lying in $\tilde{\mathcal{K}} \setminus \{\tilde{k}_{\mathrm{r}}\}$.

The *success probability* $p$ is the probability that the last-round attack outputs only the right key when the round keys are chosen independently and uniformly at random. The *key-dependent success probability* $p_{k^{(1\ldots r)}}$ is the conditional probability of this event conditioned on the event that $K^{(1..r)} = k^{(1..r)}$. Note that $p_{k^{(1..r)}}$ depends on the input block used in the attack, but the success probability $p$ is generally independent of this input block. In most cases of practical interest, $p_{k^{(1..r)}}$ is also independent of the actual value of $k^{(r)}$.

The generalization of linear cryptanalysis in [HKM95] exploits an $(r-1)$-round I/O sum $S = f(X) \oplus g(Y^{(r-1)})$ where $f$ and $g$ are balanced binary-valued functions on $\mathbb{B}^n$. The key-dependent imbalance of $S$ is defined as $I(S|k^{(1..r-1)}) := |2 \cdot P[S=0 \mid K^{(1..r-1)} = k^{(1..r-1)}] - 1|$ [HKM95]. Let $\mathcal{F}$ and $\mathcal{G}$ be the partitions whose partitioning functions are $f$ and $g$, respectively. Then, $I((\mathcal{F},\mathcal{G}) \mid k^{(1\ldots r-1)}) = I(S \mid k^{(1..r-1)})$. Thus, the last-round attack by partitioning cryptanalysis performs a last-round generalized linear cryptanalysis attack with one difference: partitioning cryptanalysis can use only half of the plaintexts, either those in $\mathcal{F}_0$ or those in $\mathcal{F}_1$, whereas the generalization of linear cryptanalysis can use all plaintexts. Since $|\mathcal{F}| = |\mathcal{G}| = 2$, this difference can be removed by modifying Steps 1 and 2 in the procedure of partitioning cryptanalysis as follows:

1'. Consider a known p/c-pair $(x, y)$ with arbitrary plaintext.

2'. For each $\tilde{k}$ in $\tilde{\mathcal{K}}$, calculate $\tilde{y}^{(r-1)} := R_{\tilde{k}}^{-1}(y)$; increment $c[k, g(\tilde{y}^{(r-1)})]$ by 1 if $x$ is in $\mathcal{F}_0$, and increment $c[k, g(\tilde{y}^{(r-1)}) \oplus 1]$ by 1 if $x$ is in $\mathcal{F}_1$.

## 4 Success Probability of Partitioning Cryptanalysis using Peak Imbalance

Partitioning cryptanalysis using peak imbalance can be applied successfully if one can find an $(r-1)$-round partition-pair $(\mathcal{F},\mathcal{G})$ and an input block $\mathcal{F}_i$ that satisfy the following conditions:

**1) Effectiveness:** $(\mathcal{F},\mathcal{G})$ is effective.

**2) Smallness of the number of key classes:** The partition $\mathcal{G}$ is such that the number $\kappa := |\tilde{\mathcal{K}}|$ of key classes is reasonably small. (The computational complexity of the attack will be proportional to this number.)

**3) Hypothesis of wrong-key randomization:** The key-dependent input-block-dependent peak imbalance $I_{\mathrm{p}}(\, g(Y^{(r-1)}) \mid f(X)=i,\ K^{(1..r-1)} = k^{(1..r-1)}\,)$ of the partition-pair $(\mathcal{F},\mathcal{G})$ for $X$ and $Y^{(r-1)}$ (i.e., for the first $r-1$ rounds) is substantially larger than the maximum over wrong keys $\tilde{k}_{\mathrm{w}}$ of this same imbalance for $X$ and the guess $R_{\tilde{k}_{\mathrm{w}}}^{-1}(Y)$ for $Y^{(r-1)}$ computed from the ciphertext $Y$ by using the wrong key $\tilde{k}_{\mathrm{w}}$ in the last round. More precisely, let the *minimum wrong-key peak imbalance decrease* be defined by

$$\begin{aligned}\Delta I_{\mathrm{p}}(k^{(1..r)}) \;:=\; & I_{\mathrm{p}}(\, g(Y^{(r-1)}) \mid f(X)=i,\ K^{(1..r-1)} = k^{(1..r-1)}\,) \\ & - \max_{\tilde{k}_{\mathrm{w}} \in \tilde{\mathcal{K}} \setminus \{k_{\mathrm{r}}\}} I_{\mathrm{p}}(\, g(R_{\tilde{K}}^{-1}(Y)) \mid f(X)=i,\ K^{(1..r)}\tilde{K} = k^{(1..r)}\tilde{k}_{\mathrm{w}}\,).\end{aligned}$$

Then, the hypothesis is that there exists a positive real number $\Delta_{\min}$, substantially larger than 0, such that, for virtually all $k^{(1..r)}$ that can result from the cipher's key scheduling algorithm, $\Delta I_{\mathrm{p}}(k^{(1..r)}) > \Delta_{\min}$.

It is insightful to consider $I_{\mathrm{p}}(\, g(R_{\tilde{K}}^{-1}(Y)) \mid f(X)=i,\ K^{(1..r)}\tilde{K} = k^{(1..r)}\tilde{k}_{\mathrm{w}}\,)$ as the key-dependent input-block-dependent imbalance of the partition-pair $(\mathcal{F},\mathcal{G})$ for an $(r+1)$-round "iterated" block cipher obtained by appending to the original cipher an $(r+1)$-th round with round function $R^{-1}$ and round key $\tilde{K}$. If $\tilde{K}$ is the right key $\tilde{k}_{\mathrm{r}}$, then the $r+1$ rounds collapse to $r-1$ rounds, and the above imbalance equals $I_{\mathrm{p}}(\, g(Y^{(r-1)}) \mid f(X)=i,\ K^{(1..r-1)} = k^{(1\ r-1)}\,)$. Otherwise, for good ciphers, we would naturally expect the $(r+1)$-round partition-pair to have substantially lower key-dependent imbalance than an $(r-1)$-round partition-pair for virtually all keys $K^{(1..r)} = k^{(1..r)}$.

By assuming hypotheses similar to those that Matsui used for approximating the success probability of linear cryptanalysis, one finds that the success probability of partitioning cryptanalysis can be approximated as

$$(1)\quad p \;\approx\; \int_{-\sqrt{N(m-1)\overline{I}_{\mathrm{r}}{}^2}}^{\infty} \tfrac{1}{\sqrt{\pi}} e^{-\frac{t^2}{2}}\, Q\Big(-(1-I)\big(t+\sqrt{N(m-1)\overline{I}_{\mathrm{r}}{}^2}\big)\Big)^{\kappa-1}\, dt$$

where $m = |\mathcal{G}|$, where $Q(\alpha) := \frac{1}{\sqrt{2\pi}} \int_{\alpha}^{\infty} e^{-\frac{t^2}{2}}\, dt$, and where $\overline{I}_{\mathrm{r}} := \overline{I}_{\mathrm{p}}(\, g(Y^{(r-1)}) \mid f(X)=i\,)$ (cf. Appendix B). This approximation gives $p$ as an increasing function of $\overline{I}_{\mathrm{r}}$, which suggests that the average-key peak imbalance $\overline{I}_{\mathrm{p}}(.)$ is a good measure for the usefulness of the partition-pair $(\mathcal{F},\mathcal{G})$.

## 5 Coset-Partition-Pairs

Since there is generally an infeasibly large number of partitions with blocks of equal sizes, we must concentrate on partitions with properties that suggest their usefulness for partitioning cryptanalysis. Many ciphers use a group operation to insert the round keys at the input of each round. For such ciphers, it is natural to consider "coset-partitions" of $\mathbb{B}^n$ with respect to this group operation.

**Definition 3.** Let "$\otimes$" be a group operation in $\mathbb{B}^n$ and $e$ the neutral element for "$\otimes$". A *coset-partition for "$\otimes$"* is a partition $\mathcal{F}$ for which the block containing $e$, $\mathcal{F}(e)$, is a subgroup of $(\mathbb{B}^n, \otimes)$ and whose other blocks are the cosets of this subgroup; i.e., a coset-partition is a partition that can be written as

$$\mathcal{F} \quad = \quad \{x \otimes \mathcal{F}(e) \,:\, x \in \mathbb{B}^n\} \ .$$

A *coset-partition-pair* is a partition-pair both of whose components are coset-partitions. A coset-partition for the component-wise XOR operation on $n$-tuples will be called a *linear partition* and a partition-pair whose input and output partitions are both linear will be called a *linear partition-pair*. The following lemma gives a fundamental property of coset-partitions.

**Lemma 4.** *Let $\phi_z$ be the automorphism $\phi_z : \mathbb{B}^n \to \mathbb{B}^n,\ x \mapsto z \otimes x$. A partition is a coset-partition for the group operation "$\otimes$" in $\mathbb{B}^n$ if and only if, for every $z$ in $\mathbb{B}^n$, the automorphism $\phi_z$ maps all elements of each block of $\mathcal{F}$ onto one block of $\mathcal{F}$, i.e., if and only if the block containing $z \otimes x$ is uniquely determined by $z$ and by the block containing $x$, or, again equivalently, if and only if $(\mathcal{F}, \mathcal{F})$ has* guaranteed transitions *for "$\otimes$", i.e., for every $\phi_z$ with $z$ in $\mathbb{B}^n$.*

## 6 Finding Effective Partition-Pairs

We now suppose that the round function $R$ of an iterated block cipher is defined by

$$Y^{(i)} \quad = \quad R_{K^{(i)}}(Y^{(i-1)}) \quad = \quad \phi(\, Y^{(i-1)} \otimes K_{\mathrm{L}}^{(i)}, K_{\mathrm{R}}^{(i)}\,) \ ,$$

where "$\otimes$" is a group operation in $\mathbb{B}^n$, where $K_{\mathrm{L}}^{(i)}$ and $K_{\mathrm{R}}^{(i)}$ denote the left and the right part of $K^{(i)}$, and where $\phi(., k_{\mathrm{R}}^{(i)})$ is invertible for all $k_{\mathrm{R}}^{(i)}$.

We propose a method for finding effective coset-partition-pairs for such ciphers. For linear cryptanalysis and the attack in [HKM95], there exists a procedure for finding effective linear expressions and effective I/O sums. With the help of Matsui's piling-up lemma, the imbalance of multi-round homomorphic I/O sums can be lower bounded in terms of the imbalances of one-round homomorphic threefold sums [HKM95]. Fortunately, the most effective I/O sums are often those for which this lower bound is the largest. For partitioning cryptanalysis, there is no general way to compute a good lower bound on the imbalance of a multi-round partition-pair given imbalances of the one-round partition-pairs that it comprises. We must

settle for *approximating* the average-key imbalance of a multi-round partition-pair.

**Piling-up hypothesis for partition-pairs.** *Consider a cascade of $\rho$ rounds with round function $R$ as defined above. Consider a list $\mathcal{F}^{(0)}, \mathcal{F}^{(1)}, \ldots, \mathcal{F}^{(\rho)}$ of coset-partitions for "$\otimes$" and let $\overline{I}^{(i)}(\mathcal{F}^{(i-1)}, \mathcal{F}^{(i)})$ be the average-key imbalance of $(\mathcal{F}^{(i-1)}, \mathcal{F}^{(i)})$ for $\phi$. Then, the average-key imbalance $\overline{I}^{(1..\rho)}((\mathcal{F}^{(0)}, \mathcal{F}^{(\rho)}))$ for $X^{(1)}$ and $Y^{(\rho)}$ can be well approximated by*

(2)

$$\tilde{I}^{(1..\rho)}((\mathcal{F}^{(0)}, \mathcal{F}^{(\rho)})) := \max \overline{I}^{(\phi)}((\mathcal{F}^{(0)}, \mathcal{F}^{(1)})) \cdot \ldots \cdot \overline{I}^{(\phi)}((\mathcal{F}^{(\rho-1)}, \mathcal{F}^{(\rho)}))$$

*where the maximum is taken over all coset-partitions $\mathcal{F}^{(1)}, \mathcal{F}^{(2)}, \ldots \mathcal{F}^{(\rho-1)}$ for $\otimes$ for which $|\mathcal{F}^{(0)}| \geq |\mathcal{F}^{(1)}| \geq \cdots \geq |\mathcal{F}^{(\rho)}|$.*

We have not been able to *prove* any result of this kind, but we have found experimentally that the "piling-up approximation" (2) is often so descriptive of the actual average-key imbalance that it can safely be used for finding effective multi-round partition-pairs.

**Procedure for finding effective $\rho$-round coset-partition-pairs**

1. Find the set $\mathcal{S}_\otimes$ of all coset-partitions for "$\otimes$".
2. For all $(\mathcal{F}, \mathcal{G})$ in $\mathcal{S}_\otimes^2$ where $|\mathcal{F}| \geq |\mathcal{G}|$, find the imbalance of the partition-pair $(\mathcal{F}, \mathcal{G})$ for the input and the output of a round. Discard the partition-pairs with small imbalance from further consideration.
3. For each $(l, m)$, where $l$ and $m$ are powers of two with $l \geq m$, consider all retained partition-pairs $(\mathcal{F}, \mathcal{G})$ in $\mathcal{S}_\otimes^2$ for the input of the first and the output of the $\rho$-th round with $|\mathcal{F}| = l$ and $|\mathcal{G}| = m$; use the piling-up approximation (2) to estimate their average-key imbalance; find the most effective such partition-pairs and their approximate average-key imbalances.
4. Use (1) to approximate the success probability of partitioning cryptanalysis. Decide for which $l$ and for which $m$ the most successful attack can be obtained.

The complexity of this procedure depends crucially on the number of coset-partitions. For cyclic group operations of $\mathbb{B}^n$, there are only $n - 2$ non-trivial coset-partitions, whereas there exist many more linear partitions. There seems to be little chance of finding an effective partition-pair for ciphers using cyclic group operations on $\mathbb{B}^n$ and partitioning cryptanalysis seems not to be powerful against such ciphers. For ciphers using bitwise XOR to insert the keys, there are so many coset-partitions that it is generally infeasible to compute the maximum specified in the piling-up hypothesis.

## 7 Partitioning Cryptanalysis of DES

We applied the last-round attack by partitioning cryptanalysis to six rounds of the Data Encryption Standard (DES). Details of this attack are given in Appendix C.

For a certain partition-pair, we analyzed in our attack all 256 p/c-pairs with plaintexts in one input block. The success probability was about 95% for partitioning cryptanalysis using the Euclidean imbalance but was only 74% for partitioning cryptanalysis using the peak imbalance [Har96]. Our better success probability is about the same as that obtained by Biham and Shamir for differential cryptanalysis of 6-round DES (i.e., a success probability of 95% using 240 p/c-pairs with chosen plaintexts [BS93, page 31]), and it is slightly worse than the attack of [Knu95], but a new weakness of 6-round DES is exploited in partitioning cryptanalysis.

## 8 Conclusions

Partitioning cryptanalysis of iterated block ciphers was introduced. This is a generalization of linear cryptanalysis and exploits a weakness that can be described by an effective partition-pair, i.e., a pair of partitions such that, for every key, the next-to-last-round outputs are substantially non-uniformly distributed over the blocks of the second partition when the plaintexts are chosen uniformly from a particular block of the first partition. The success probability of partitioning cryptanalysis was approximated by assuming hypotheses similar to those that Matsui assumed to estimate the success probability of linear cryptanalysis. The crucial problem of partitioning cryptanalysis, namely the problem of finding effective partition-pairs, was addressed. Our procedure for finding effective coset-partition-pairs requires extensive computation for ciphers in which the round keys are inserted with the XOR operation. When the keys are inserted with group operations for large cyclic groups, our procedure is considerably faster, but the chance to find an effective partition-pair is generally small. To illustrate the potential usefulness of partitioning cryptanalysis, we applied it to DES. For 6-round DES, attacks by partitioning cryptanalysis are chosen-plaintext attacks that are about as successful as differential cryptanalysis, although they are based on a different weakness. We close by remarking that ciphers that are very weak against partitioning cryptanalysis, but quite strong against both linear and differential cryptanalysis have been designed in [Har96].

## References

[BS93] Eli Biham and Adi Shamir. *Differential Cryptanalysis of the Data Encryption Standard.* Springer, New York, 1993. ISBN 3-540-97930-1.

[Har96] Carlo Harpes. *Cryptanalysis of iterated block ciphers*, volume 7 of *ETH Series in Information Processing.* Hartung-Gorre Verlag Konstanz, J. L. Massey editor, 1996. ISBN 3-89649-079-6.

[Har94] Carlo Harpes. *Success probability of partitioning cryptanalysis.* In H. C. A. van Tilborg and F. M. J. Willems, editors, *Proceedings of the EIDMA Winter Meeting on Coding Theory, Information Theory and Cryptology.* December 1994.

[HKM95] Carlo Harpes, Gerhard G. Kramer, and James L. Massey. A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma. In L. C. Guillou and J.-J. Quisquater, editors, *Advances in Cryptology – Eurocrypt '95*, Lecture Notes in Computer Science No. 921, pages 24–38. Springer, 1995.

[KR95] Burton S. Kaliski and Matthew J. B. Robshaw. Linear cryptanalysis using multiple approximations. In A. De Santis, editor, *Advances in Cryptology – Eurocrypt '94*, Lecture Notes in Computer Science No. 950, pages 26–39. Springer, 1995.

[Knu95] Lars Knudsen. Truncated and high order differentials. In B. Preneel, editor, *Fast Software Encryption*, Lecture Notes in Computer Science No. 1008, pages 196–211. Springer, 1995.

[Mat94a] Mitsuru Matsui. The first experimental cryptanalysis of the Data Encryption Standard. In Y. G. Desmedt, editor, *Advances in Cryptology – Crypto '94*, Lecture Notes in Computer Science No. 839, pages 1–11. Springer, 1994.

[Mat94b] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology – Eurocrypt '93*, Lecture Notes in Computer Science No. 765, pages 386–397. Springer, 1994.

[MPWW94] Sean Murphy, Fred Piper, Michael Walker, and Peter Wild. Likelihood estimation for block cipher keys. Submitted for publication, May 1994.

[Vau96] Serge Vaudenay. An experiment on DES: Statistical Cryptanalysis. In *Proceedings of the 3rd ACM Conferences on Computer Security*, pages 139–147. ACM Press, 1996.

## A Combined Partitioning Cryptanalysis

Partitioning cryptanalysis is a chosen-plaintext attack because only p/c-pairs with plaintexts from one input block can be considered, but any input block in $\mathcal{F}$ can generally be used. We may extend partitioning cryptanalysis to form a known-plaintext attack by combining partitioning cryptanalysis attacks that use different input blocks in the following way.

0. Set up a counter $c[i, \tilde{k}, j]$ for each $i$ such that $0 \le i < l$, for each $j$ such that $0 \le j < m$, and for each $\tilde{k}$ in $\tilde{\mathcal{K}}$; and initialize all counters to 0.
1. Choose a known p/c-pair $(x, y)$ with arbitrary plaintext.
2. For each $\tilde{k}$ in $\tilde{\mathcal{K}}$, calculate $\tilde{y}^{(r-1)} := R_{\tilde{k}}^{-1}(y)$ and increment $c[f(x), \tilde{k}, g(\tilde{y}^{(r-1)})]$ by 1.
3. Repeat Steps 1 and 2 for all known p/c-pairs.
4. For each $i$ such that $0 \le i < l$ and each $\tilde{k}$ in $\tilde{\mathcal{K}}$, reorder the values of the counters $c[i, \tilde{k}, 0]$, $c[i, \tilde{k}, 1], \ldots, c[i, \tilde{k}, m-1]$ so that $c[i, \tilde{k}, 0] \ge \ldots \ge c[i, \tilde{k}, m-1]$.
5. For each $\tilde{k}$ in $\tilde{\mathcal{K}}$ and each $j$ such that $0 \le j < m$, set $c'[\tilde{k}, j] = \sum_{i=0}^{l-1} c[i, \tilde{k}, j]$.
6. Output the key(s) $\tilde{k}$ maximizing $\hat{\mu}(\tilde{k}) = I(\frac{c'[\tilde{k},0]}{N}, \frac{c'[\tilde{k},1]}{N}, \ldots, \frac{c'[\tilde{k},m-1]}{N})$ as candidate(s) for the key actually used in the last round.

We will call this attack *combined partitioning cryptanalysis* (CPC). The combined partitioning cryptanalysis attack is similar to the attack by linear cryptanalysis using multiple approximations [KR95]. Note that combined partitioning cryptanalysis is a known-plaintext attack and that it will not be successful if $l$ is large as there will be generally too few p/c-pairs with plaintexts in the same input block unless the plaintexts have been chosen such that they lie in a small number of input blocks. The complexity of the attack is considerably reduced if peak imbalance is used.

## B Approximation of the Success Probability

We assume that the imbalance used in partitioning cryptanalysis is the peak imbalance $I_{\mathrm{p}}(.)$. We first propose a model of how the various counters in the last-round attack increment. Let $\tilde{J}(\tilde{k})$ denote the random variable indicating which counter is incremented for the key guess $\tilde{k}$ when a certain p/c-pair is analyzed, i.e., $\tilde{J}(\tilde{k}) = g(\tilde{Y}^{(r-1)}(\tilde{k}))$, and let $J = g(Y^{(r-1)})$ indicate which counter is incremented for the right key $\tilde{k}_{\mathrm{r}}$.

**Model for counter incrementing.** *For each wrong key $\tilde{k}_{\mathrm{w}}$ in $\tilde{\mathcal{K}} \setminus \{\tilde{k}_{\mathrm{r}}\}$, independently for all $\tilde{k}_{\mathrm{w}}$, $\tilde{J}(\tilde{k}_{\mathrm{w}})$ is the output of an $m$-ary symmetric channel with dominant probability $q$, where $q \geq \frac{1}{m}$, and input $J$, where $J = \tilde{J}(\tilde{k}_{\mathrm{r}})$, i.e.,*

$$P[\,\tilde{J}(\tilde{k}_{\mathrm{w}}) = \tilde{\jmath} \mid J = j\,] \quad = \quad \begin{cases} q & \text{if } \tilde{\jmath} = \pi_{\tilde{k}_{\mathrm{w}}}(j) \\ \frac{1-q}{m-1} & \text{if } \tilde{\jmath} \neq \pi_{\tilde{k}_{\mathrm{w}}}(j) \end{cases},$$

*where $\pi_{\tilde{k}_{\mathrm{w}}}$ is some permutation of $\{0, 1, \ldots, m-1\}$. Moreover, $q = \frac{m-1}{m} I + \frac{1}{m}$ and $I$, which will be called the* imbalance *of the $m$-ary symmetric channel with dominant probability $q$, is well approximated as*

$$I \quad \approx \quad \frac{E[\,I_{\mathrm{p}}(J(\tilde{K}_{\mathrm{w}}))\,]}{I_{\mathrm{p}}(J)} \,. \tag{3}$$

The parameter $I$ or, equivalently, the parameter $q$, characterizes the randomization caused by the last round.

To find $I$ in partitioning cryptanalysis using peak imbalance, we may approximate $I_{\mathrm{p}}(J)$ and $I_{\mathrm{p}}(\tilde{J}(\tilde{k}_{\mathrm{w}}))$ by obvious estimates, namely by the empirical decision metrics $\hat{\mu}(\tilde{k}_{\mathrm{r}})$ and $\hat{\mu}(\tilde{k}_{\mathrm{w}})$, respectively. Moreover, if we assume that $I_{\mathrm{p}}(\tilde{J}(\tilde{k}_{\mathrm{w}})) \approx E[\,I_{\mathrm{p}}(J(\tilde{K}_{\mathrm{w}}))\,]$ for all $\tilde{k}_{\mathrm{w}}$, then (3) follows from the following lemma.

**Lemma 5.** *Let the random variable $J$ be the input to an $m$-ary symmetric channel with dominant probability $q$ or, equivalently, with imbalance $I = \frac{m}{m-1}(q - \frac{1}{m})$, and let $\tilde{J}(\tilde{k}_{\mathrm{w}})$ be the output. Then, for any probability distribution for $J$,*

$$I_{\mathrm{p}}(\tilde{J}(\tilde{k}_{\mathrm{w}})) \quad = \quad I_{\mathrm{p}}(J) \cdot I \,.$$

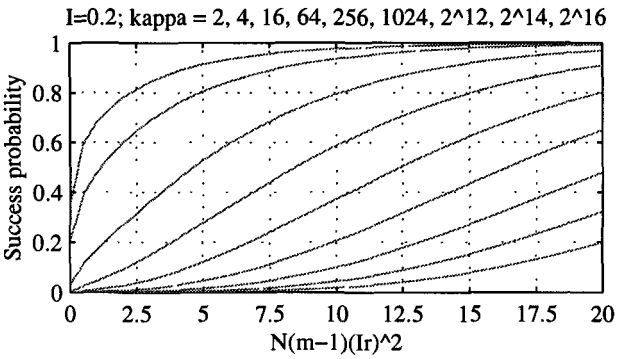
Note that if the model for counter incrementing is satisfied for an effective partition-pair and if $I$ is substantially smaller than 1, then the hypothesis of wrong-key randomization is also fulfilled. The following theorem is based on the given model for counter incrementing and provides a good approximation of the success probability of partitioning cryptanalysis.

**Theorem 6. (Success probability of partitioning cryptanalysis)** *Consider the last-round attack by partitioning cryptanalysis for the partition-pair $(\mathcal{F},\mathcal{G})$, using peak imbalance, analyzing $N$ p/c-pairs with plaintexts in an input block $\mathcal{F}_i$, and distinguishing $\kappa$ key classes. Suppose first that $N$ is sufficiently large. Suppose second that the above model for counter incrementing holds. Suppose third that, for each of the $\kappa$ key guesses, the count that is the most likely to be incremented dominates the other counts. Then, the success probability of this attack, when the key in use is $k^{(1..r)}$, is well approximated by*

$$(4)\quad p_{k^{(1..r)}} \approx \int_{-\sqrt{N(m-1)I_r^2}}^{\infty} \frac{1}{\sqrt{\pi}} e^{-\frac{t^2}{2}} Q\Big(-(1-I)(t+\sqrt{N(m-1)I_r^2})\Big)^{\kappa-1} dt \ ,$$

*where $m = |\mathcal{G}|$, where $Q(\alpha) := \frac{1}{\sqrt{2\pi}} \int_{\alpha}^{\infty} e^{-\frac{t^2}{2}} dt = \frac{1}{2}(1 - \mathrm{erf}(\frac{\alpha}{\sqrt{2}}))$, and where $I_r$ is the key-dependent input-block-dependent imbalance of $(\mathcal{F},\mathcal{G})$ for the first $r-1$ rounds given that $\mathcal{F}_i$ is the input block used in the attack and that $K^{(1..r-1)} = k^{(1..r-1)}$.*

In the following figure, we show the approximate success probability as a function of $N(m-1)I_r^2$ for different values of $\kappa$ and $I$, where $I$ is well estimated by the quotient of the wrong-key and the right-key empirical decision metrics.




Now, if for virtually all keys $k^{(1..r-1)}$ in $\mathcal{K}^{r-1}$ and for all $i$, $0 \le i < l$,

$$I_{\mathrm{p}}(g(Y^{(r-1)}) \mid f(X)=i,\ K^{(1..r-1)} = k^{(1..r-1)}) \quad \approx \quad \overline{I}_{\mathrm{p}}(g(Y^{(r-1)}) \mid f(X)=i)$$

— this assumption may be called the *hypothesis of fixed-key equivalence in partitioning cryptanalysis* — then (1) follows. In practice, however, the hypothesis of fixed-key equivalence for partitioning cryptanalysis is generally not well satisfied. We observe that the approximation on the right of (1) is often a convex-U

function of the key-dependent imbalance $I_r$ for small imbalances and a convex-$\cap$ (or concave) function of $I_r$ for large imbalances. By Jensen's inequality, we then expect this approximation to be smaller than the true success probability when the key-dependent imbalances are low (or, equivalently, when the success probability is low) and vice versa. We now confirm these expectations for DES.

## C Partitioning Cryptanalysis of DES

A linear partition $\mathcal{F}$ can be described by a *parity-check matrix* $H_{\mathcal{F}}$ whose rows are the $n$-tuples $\alpha_1, \alpha_2, \ldots, \alpha_d$. Given $H_{\mathcal{F}}$, the partition $\mathcal{F}$ is the set of cosets of the linear code $\mathcal{F}(0)$ for which $H_{\mathcal{F}}$ is a parity-check matrix, i.e., $\mathcal{F}$ is the set of cosets of the subgroup $\mathcal{F}(0) = \{x : x \in \mathbb{B}^n, xH_{\mathcal{F}}^{\mathrm{T}} = 0\}$. The partitioning function of $\mathcal{F}$ can be chosen as $f : x \mapsto xH_{\mathcal{F}}^{\mathrm{T}}$. The parity-check matrix $H_{\mathcal{F}}$ is called *reduced* if its rows are linearly independent. In this case, the blocks of $\mathcal{F}$ can be labeled with $d = \log_2(|\mathcal{F}|)$ binary digits.

A linear partition with parity-check matrix $H_{\mathcal{F}}$ such that the Hamming weight of each row is 1 will be called *bit-selecting*. Its subgroup can be written as $\mathcal{F}(0) = \{x : x \in \mathbb{B}^n, \alpha \& x = 0\}$ for some $n$-tuple $\alpha$ with Hamming weight $d$, where "&" denotes bitwise AND and 0 represents the all-zero $n$-tuple. The $n$-tuple $\alpha$ will be called the *bit-selecting $n$-tuple* of $\mathcal{F}$. The $i$-th bit of a bit-selecting $n$-tuple $\alpha$ will be called *constrained by* $\mathcal{F}$ if the $i$-th bit of $\alpha$ is 1, and called *free* otherwise. A block of a linear partition is uniquely determined by specifying the constrained bits for an element of this block.

Our procedure for finding effective partition-pairs for DES is similar to the procedure given in Section 6, but we use a simpler approximation of the partition-pair average-key imbalances. Since it is infeasible for 5-round DES to compute the product in (2) for all lists $(\mathcal{F}^{(0)}, \mathcal{F}^{(1)}, \ldots, \mathcal{F}^{(5)})$ such that $|\mathcal{F}^{(0)}| \geq |\mathcal{F}^{(1)}| \geq \cdots \geq |\mathcal{F}^{(5)}|$, we reduce the number of lists $(\mathcal{F}^{(0)}, \mathcal{F}^{(1)}, \ldots, \mathcal{F}^{(5)})$ for which we actually compute the product as follows. The S-boxes from which constrained bits emerge will be called *active*. We restricted ourselves to lists of bit-selecting linear partitions in which all bits that connect active S-boxes are constrained. Moreover, we used an appropriate approximation for the one-round partition-pair peak imbalances. Our procedure provided us with many effective partition-pairs. We empirically computed the peak imbalances of the most effective partition-pairs found and we verified that the empirical peak imbalance depends on the imbalance estimated in our procedure (cf. Fig. 3 left), which shows that the imbalance estimate can be used for finding effective partition-pairs. We then approximated the success probability of attacks exploiting these partition-pairs, performed the attacks many times, and empirically estimated the success probability.

In Fig. 3 (right), we compared the approximate success probability and the empirically estimated success probability. Note that to evaluate (1), $I$ is given by (3) in which the peak imbalances are replaced by empirical estimates of average-key peak imbalances. The difference between the quantities shown in Fig. 3 can be explained mainly by the fact that the hypothesis of fixed-key equivalence is not well satisfied (cf. Appendix B). Thus, our results suggest that Theorem 6 gives a

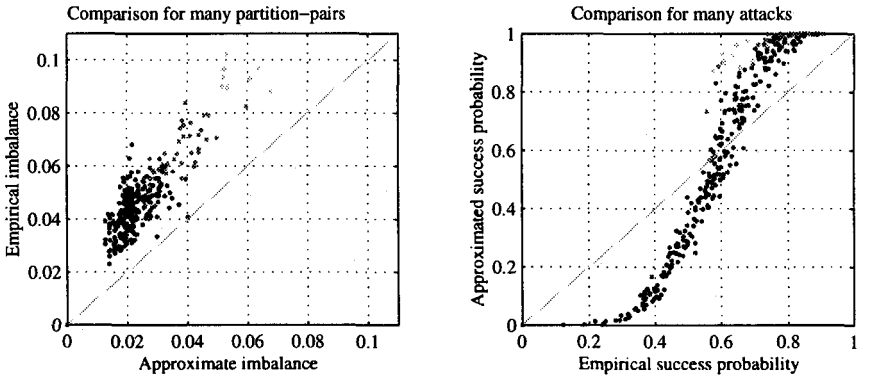



**Fig. 3.** Left: comparison of the approximate imbalances to the empirical imbalances of partition-pairs for 5-round DES; right: comparison of the empirical success probability and the approximate success probability of partitioning cryptanalysis using the peak imbalance for 6-round DES. For many attacks all using different partition-pairs whose input partition has $2^{64-l^*}$ blocks where $l^* = 8$ (light-grey points), 10, 12, or 14 (dark points), the empirical partition-pair imbalance and the empirical success probability are estimated after attacking 100 000 random keys. The number of known p/c-pairs in the attacks was $N = 256$ for $l^* = 8$ and $N = 1024$ otherwise.

good approximation to the true success probability, although the approximation (1) may be crude.

We also performed attacks by partitioning cryptanalysis using different imbalance measures. Partitioning cryptanalysis attacks using Euclidean imbalance were generally slightly stronger than attacks using peak imbalance.

The most successful partitioning cryptanalysis attack on 6-round DES using 256 chosen p/c-pairs was obtained when the attack used Euclidean imbalance, when the bit-selecting 64-tuple of the input partition was `81fff9ff ffffffff` and when the bit-selecting 64-tuple of the round four output partition was `00000000 0000f000` (i.e., when the output block was defined only by the bits that are linked to the S-box S5 of the fourth round). The approximate imbalance computed in the procedure for finding effective bit-selecting linear partition-pairs is then 0.0638 and the empirical imbalance is 0.0970. The empirical success probability is 95% for partitioning cryptanalysis using Euclidean imbalance but is only 74% for partitioning cryptanalysis using peak imbalance when all 256 p/c-pairs with plaintexts in one block are used. According to our approximation with $q$ empirically determined as 0.39, the latter success probability should be 95% instead of 74%, which indicates that the approximation is good for most purposes.