# A Model for Structure Attacks, with Applications to PRESENT and Serpent

Meiqin Wang[1,2,3,⋆], Yue Sun[4], Elmar Tischhauser[2,3,⋆⋆], and Bart Preneel[2,3]

[1] Key Laboratory of Cryptologic Technology and Information Security,
Ministry of Education, Shandong University, Jinan 250100, China
[2] Department of Electrical Engineering ESAT/SCD-COSIC,
Katholieke Universiteit Leuven, Kasteelpark Arenberg 10, B-3001 Heverlee, Belgium
[3] Interdisciplinary Institute for BroadBand Technology (IBBT), Belgium
[4] Institute for Advanced Study, Tsinghua University, Beijing 100084, China
mqwang@sdu.edu.cn

**Abstract.** As a classic cryptanalytic method for block ciphers, hash functions and stream ciphers, many extensions and refinements of differential cryptanalysis have been developed. In this paper, we focus on the use of so-called structures in differential attacks, *i.e.* the use of multiple input and one output difference. We give a general model and complexity analysis for structure attacks and show how to choose the set of differentials to minimize the time and data complexities. Being a subclass of multiple differential attacks in general, structure attacks can also be analyzed in the model of Blondeau *et al.* from FSE 2011. In this very general model, a restrictive condition on the set of input differences is required for the complexity analysis. We demonstrate that in our dedicated model for structure attacks, this condition can be relaxed, which allows us to consider a wider range of differentials. Finally, we point out an inconsistency in the FSE 2011 attack on 18 rounds of the block cipher PRESENT and use our model for structure attacks to attack 18-round PRESENT and improve the previous structure attacks on 7-round and 8-round Serpent. To the best of our knowledge, those attacks are the best known differential attacks on these two block ciphers.

**Keywords:** Structure Attack, Block Cipher, Differential, PRESENT, Serpent.

## 1 Introduction

Differential cryptanalysis [2] is a classic cryptanalytic method that has been successfully applied to block ciphers, hash functions and stream ciphers. The key

[⋆] This author is supported by 973 Project (No.2007CB807902), National Natural Science Foundation of China (Grant No.61133013, No.61070244 and No.60931160442), Outstanding Young Scientists Foundation Grant of Shandong Province (No.BS2009DX030), Shandong University Initiative Scientific Research Program (2009TS087)

[⋆⋆] Elmar Tischhauser is a research assistant of the F.W.O., Fund for Scientific Research — Flanders.

A. Canteaut (Ed.): FSE 2012, LNCS 7549, pp. 49–68, 2012.

step for a differential attack is to identify a differential characteristic with high probability as a distinguisher, then use it to recover (part of) the key. Lai *et al.* propose the notion of *differential* which encompasses the collection of all possible differential characteristics [13] for one fixed input and output difference. A lower bound for the probability of a differential (and thus, an upper bound for the complexity of the attack) can be obtained by combining the probabilities of a number of differential characteristics belonging to the differential. Therefore, differentials give a better estimation of the actual attack complexity than characteristics, since the distinguisher can exploit any characteristic belonging to the differential. In order to further improve differential attacks, multiple differentials with a single output difference but multiple input differences can be used. This can reduce the data complexity provided that the set of input differences for the differentials can be combined in a so-called *structure*. Therefore, we call this type of differential attacks *structure attacks*. The structure technique in differential cryptanalysis was originally introduced in a more restrictive way as *quartets* to attack DES [2], and multiple differential characteristics with multiple input differences and a single output difference have been used to attack DES. In addition, Biham *et al.* use the structure technique to attack reduced-round versions of the Serpent block cipher [3].

At FSE 2011, Blondeau *et al.* proposed multiple differential cryptanalysis with multiple input differences and multiple output differences [4] and gave an explicit formula to compute the success probability of multiple differential cryptanalysis. Traditionally, a normal approximation to the binomial distribution was used to evaluate the success probability of a differential attack [18,19]. The approach of [4] provides a more accurate estimation of the success probability. Since structure attacks are a special case of multiple differential cryptanalysis, those results also apply to our structure attacks.

However, in order to ensure that one pair of ciphertexts can be only counted once, the model of [4] requires a certain condition to be met (see Definition 1), which severely restricts the set of input difference values that can be used in an attack. In this paper, we demonstrate that this condition on the set of the input difference values is so strong that many valuable differentials may be excluded. We show that in the structure technique, this condition can be relaxed without counting ciphertexts more than once. This enables us to choose our differentials more freely, leading to improved attack complexities.

We stress that this condition and the general model of [4] are still necessary for the analysis of the general case where one has multiple input and multiple output differences. What we propose in this paper, is a tailored model for structure attacks, which are an important and often particularly efficient subclass of multiple differential cryptanalysis.

Furthermore, the multiple differential attack on 18-round PRESENT [4] uses 561 differentials with 17 input differences and 33 output differences [5]. It turns out that the sum of the probabilities of those 561 differentials is not correct in [4]. When calculated correctly, however, the obtained probability is lower than the random probability, implying that this set of 561 differentials cannot be used in an attack. Finally, we compare our attack to the corrected version [6] of the attack of [4].

In order to evaluate the resistance of a block cipher to differential cryptanalysis, it is crucial to take into account the effect of combining multiple differentials. However, it is often not clear a priori which choice of differentials can actually lead to an improvement. Compared to classic differential cryptanalysis with one differential, a structure attack can obviously reduce the data complexity. In order to reduce the overall time complexity, however, the differentials have to be chosen carefully.

In this paper, we first present a general model for structure attacks, providing guidance on how to choose the differentials to minimize the time complexity. Secondly, we demonstrate structure attacks for 18-round PRESENT-80 with a data complexity of $2^{64}$ chosen plaintexts and time complexity of $2^{76}$ 18-round encryptions. We find that the properties of differentials in PRESENT cause structure attacks to be more efficient than the multiple differential cryptanalysis proposed in [4]. Thirdly, we improve the differential cryptanalytic result for the block cipher Serpent. In [3], Biham *et al.* describe a differential attack for 7-round Serpent with a data complexity of $2^{84}$ chosen plaintexts and a time complexity of $2^{85}$ memory accesses. Biham *et al.* also give a differential attack on 8-round Serpent-256 with $2^{213}$ memory accesses and $2^{84}$ chosen plaintexts. In our attack for 7-round Serpent, the data complexity is reduced to $2^{71}$ chosen plaintexts and the time complexity is $2^{74.99}$ encryptions. The attack can be further extended to 8-round Serpent-256. The time complexity is then increased to $2^{203.81}$ encryptions, with the data complexity remaining at $2^{71}$ chosen plaintexts.

For PRESENT-80, the best known attack is the linear hull cryptanalysis of 26-round PRESENT [8]. For Serpent-128, the best known cryptanalytic result is the differential-linear cryptanalysis on 12 rounds [12]. Although our attacks do not improve on those results for PRESENT and Serpent, to the best of our knowledge, they are the best *differential* attacks for PRESENT and Serpent. Moreover, our proposed attack model can be used to improve differential cryptanalytic results on other block ciphers as well.

This paper is organized as follows. Section 2 briefly describes the method for computing the success probability with multiple differentials. Section 3 introduces the structure attack model and the probability distribution of the key under multiple differentials. In Sect. 4, we demonstrate the attack for 18-round PRESENT. In Sect. 5, the improved attacks on 7-round and 8-round Serpent are presented. Section 6 concludes the paper.

## 2 Brief Description of Blondeau *et al.'s* Multiple Differential Cryptanalysis

In [4], Blondeau *et al.* propose multiple differential cryptanalysis using multiple differentials with different input differences and different output differences and give a precise analytical model to compute the success probability. In [18], Selçuk uses a Gaussian approximation of the binomial distribution to derive a formula for the success probability for differential cryptanalysis. Since then, his formula has been used in many papers on differential cryptanalysis. Blondeau *et al.* demonstrate that Selçuk's method cannot be applied to multiple differential cryptanalysis and express the distribution of key counters instead in terms of a hybrid distribution including the Kullback-Leibler divergence and a Poisson distribution [4]. Blondeau *et al.* obtain the following formula for the success probability $P_S$:

$$P_S \approx 1 - G_*[G^{-1}(1 - \tfrac{l-1}{2^{n_k}-2}) - 1/N_s], \tag{1}$$

where $n_k$ is the number of key candidates, $l$ is the size of the list to keep, $G$ is defined by $G^{-1}(y) = \min\{x|G(x) \geq y\}$, and $N_s$ is the number of samples. Note that (1) corrects a typo in [4] by dividing by $N_s$ for normalization. The functions $G$ and $G_*$ are defined as $G_*(\tau) \overset{\text{def}}{=} G(\tau, p_*)$ and $G(\tau) \overset{\text{def}}{=} G(\tau, p)$, where $p_* = \frac{\sum_{i,j} p_*^{(i,j)}}{|\Delta_0|}$ and $p = \frac{|\Delta|}{2^m|\Delta_0|}$. $p_*^{(i,j)}$ is the probability for the differential with the $i$-th input difference value and the $j$-th output difference value, $m$ is the block size, $|\Delta_0|$ is the number of input difference values and $|\Delta|$ is the number of differentials. $G(\tau, p_*)$ and $G(\tau, p)$ can be calculated with the following equations:

$$G(\tau, q) \overset{\text{def}}{=} \begin{cases} G_-(\tau, q) & \text{if} \quad \tau < q - 3 \cdot \sqrt{q/N_s}, \\ 1 - G_+(\tau, q) & \text{if} \quad \tau > q + 3 \cdot \sqrt{q/N_s}, \\ G_{\mathcal{P}}(\tau, q) & \text{otherwise}, \end{cases} \tag{2}$$

where $G_{\mathcal{P}}(\tau, q)$ is the cumulative distribution function of the Poisson distribution with parameter $qN_s$. $G_-(\tau, q)$ and $G_+(\tau, q)$ are defined as follows:

$$\begin{aligned} G_-(\tau, q) &\overset{\text{def}}{=} e^{-N_s D(\tau \| q)} \cdot [\tfrac{q\sqrt{1-\tau}}{(q-\tau)\sqrt{2\pi\tau N_s}} + \tfrac{1}{\sqrt{8\pi\tau N_s}}], \\ G_+(\tau, q) &\overset{\text{def}}{=} e^{-N_s D(\tau \| q)} \cdot [\tfrac{(1-q)\sqrt{\tau}}{(\tau-q)\sqrt{2\pi N_s(1-\tau)}} + \tfrac{1}{\sqrt{8\pi\tau N_s}}], \end{aligned} \tag{3}$$

where $D(\tau\|q)$ is the Kullback-Leibler divergence defined by $D(\tau\|q) \overset{\text{def}}{=} \tau \ln\left(\frac{\tau}{q}\right) + (1-\tau)\ln\left(\frac{1-\tau}{1-q}\right)$.

**On the Assumptions for This Analysis.** In order to guarantee that each pair is counted only once, Blondeau *et al.* give Definition 1 as a necessary condition for the set of the input differences $\Delta_0$.

**Definition 1.** *The set of input differences $\Delta_0$ is admissible if there exists a set $\chi$ of $N/2$ plaintexts that fulfils the condition:*

$$\forall \delta_0^{(i)} \in \Delta_0, \forall x \in \chi, x \oplus \delta_0^{(i)} \notin \chi, \tag{4}$$

where $N$ is the number of chosen plaintexts. However, this condition is so strong that many differentials will be excluded. For example, independent of the algorithm under consideration, the set of input differences $\Delta_0 = \{1_x, 2_x, 3_x\}$ is never admissible in any substitution-permutation network (SPN) because of this condition, since the overlapping bits of $3_x = 1_x \oplus 2_x$ will always result in double-counting.

By contrast, in the structure technique, we can use a hash table to exclude the duplicate pair arising from the violation of Definition 1. In fact, making use of hash tables, structure attacks can use more differentials while still ensuring that each pair is counted only once. Since we only have one possible output difference, this also enables the use of the complexity analysis of [4] for sets of plaintexts not satisfying Def. 1: This condition is only necessary to avoid counting both $x$ and $x \oplus \delta_0^{(i)}$ for any $\delta_0^{(i)} \in \Delta_0$, i.e. guarantee $N_s = N|\Delta_0|/2$. This is satisfied in our approach, since each hash table will produce $N/2$ plaintext pairs with one input difference from $N$ plaintexts, in total therefore $N_s = |\Delta_0|N/2$ plaintext pairs with $|\Delta_0|$ input diffference values. For structure attacks, the complexity analysis of [4] is therefore applicable independent of Def. 1.

This has additionally been verified by experiments on SmallPresent with block length of 24 bits, 12 rounds, and a set of 11 differentials with input differences violating Definition 1 and a single output difference.

**On Previous Attacks on 18-Round PRESENT.** There are two previously published differential attacks on 18-round PRESENT [4,6]. In this section, we point out two inconsistencies in both attacks, and demonstrate that our attack compares favourably to them.

In [4], a multiple differential attack for 18-round PRESENT is presented. They identify 561 differentials[1] including 17 input differences and 33 output differences using a branch-and-bound algorithm. In [4], the probabilities $p_*$ and $p$ are calculated as $p_* = \frac{\sum_{i,j} p_*^{(i,j)}}{|\Delta_0|} = 2^{-58.50}$ and $p = \frac{|\Delta|}{2^m|\Delta_0|} = 2^{-64} \cdot 33 = 2^{-58.96}$. However, the value of $p_*$ is not correct; it should be $p_* = 2^{-60.39}$, which is less than the random probability for 33 output differences $p = 2^{-58.96}$. We found that even when one choses an optimal subset of these 561 differentials, this attack compares unfavourably to our structure attack.

In [6], another multiple differential attack on 18-round PRESENT is presented. It can be seen from Table 4 of [6], that $|\Delta_0| = 17$ (and not 16 as assumed in the paper). This results in $p_* = 2^{-62.6765}$ (instead of $2^{-62.59}$) and $p = 2^{-63.56}$ (instead of p=$2^{63.47}$). Based on these values, we compare this attack to our attack from Sect. 4 for different values of the number $\ell$ of remaining key candidates:

| Attack of [6] | | Attack of Sect. 4 | | | |
|---|---|---|---|---|---|
| $\ell$ | $P_S$ | $\ell$ | $P_S$ | $N$ | time complexity |
| $2^{38}$ | 65.27% | $2^{36}$ | 85.94% | $2^{64}$ | $2^{76}$ |
| $2^{39}$ | 79.68% | $2^{37}$ | 92.30% | $2^{64}$ | $2^{77}$ |
| $2^{41}$ | 94.62% | $2^{39}$ | 98.36% | $2^{64}$ | $2^{79}$ |

[1] These differentials have been obtained through private communication with Blondeau *et al.*

One can see that for the same data and time complexities, the structure attack performs consistently better than multiple differential cryptanalysis with multiple input differences and multiple output differences. This implies that PRESENT is not a good example to show the efficiency of multiple differential cryptanalysis with different input differences and different output differences.

## 3 Structure Attack

### 3.1 Principle of the Attack

The structure attack is a form of differential cryptanalysis which uses multiple input differences and a single output difference. Structure attacks are a special case of multiple differential cryptanalysis, but their form allows for a dedicated attack procedure, which we describe in this section.

A structure attack is performed in three phases:

1. **Data Collection Phase:** Collect a large number of ciphertext pairs with the differences produced from the output difference of the differentials and the corresponding plaintext differences belong to the set of the input differences.
2. **Data Analysis Phase:** Derive the list of the best candidates for some key bits from the collected ciphertext pairs.
3. **Key Search Phase:** Search the list of candidates and all the corresponding master keys (*i.e.*, the unexpanded key from which the round subkeys are derived).

The idea of the structure attack is to use more differentials with multiple input differences and a single output difference to reduce the data complexity. However, the set of the input differences must be controlled in order to reduce the time complexity. This is done by organizing the plaintext in so-called *structures*:

**Definition 2.** *Let* $\{\Delta_0^1, \ldots, \Delta_0^t\}$ *be a set of* $t$ *input differences. A collection of plaintexts of the form*

$$\bigcup_x \{x \oplus \Delta \mid \Delta \in \mathrm{span}\{\Delta_0^1, \ldots, \Delta_0^t\}\}, \tag{5}$$

*with* span *denoting the linear span operator, is called a* structure*.*

In this way, we can construct structures to produce the expected number of right pairs with lower data complexity compared with a single differential. Now we will give a model to choose the differentials to reduce the complexity. For clarity of exposition, we describe the model for the case of a substitution-permutation network (SPN); however, the concept can analogously be applied to other block cipher constructions, most importantly Feistel ciphers.

If we attack an $R$-round block cipher with $|\Delta_0|$ $r$-round differentials with a single output difference and multiple input differences, we denote these differentials as follows:

$$\Delta_0^i \xrightarrow{r} \Delta_r,\ \mathit{Probability} = p_i,\ (1 \le i \le |\Delta_0|),$$

where $\Delta_0^i$ and $\Delta_r$ are the $i$-th input difference and the output difference, respectively. The following notations are related with the attack:

- $m$: the block size of the block cipher.
- $k$: the key size of the block cipher.
- $|\Delta_0|$: the number of differentials.
- $p_i$: the probability of the differential with input difference $\Delta_0^i$.
- $N_{st}$: the number of structures is $2^{N_{st}}$.
- $N_p$: the number of plaintexts bits involved in the active S-boxes in the first round for all differentials.
- $N_c$: the number of ciphertexts bits involved in the non-active S-boxes in the last round deriving from $\Delta_r$.
- $\beta$: the filtering probability for the ciphertext pairs.
- $p_f$: the filtering probability for the ciphertext pairs according to active S-boxes, $p_f = \beta \cdot 2^{N_C}$.
- $l$: the size of the candidate list.
- $n_k$: the number of guessed subkey bits in the last $R - r$ rounds.

In the attack, $2^{N_{st}}$ structures are constructed. In each structure, all the input bits to non-active S-boxes in the first round are fixed to some random value, while $N_p$ input bits of all active S-boxes take all $2^{N_p}$ possible values. There are $2^{N_{st}} \cdot 2^{N_p - 1} = 2^{N_{st}+N_p-1}$ pairs for each differential. We expect that about $2^{N_{st}+N_p-1} \cdot \sum_{i=1}^{|\Delta_0|} p_i$ pairs produce the output difference $\Delta_r$. These pairs are right pairs.

The attack is described as follows.

1. For each structure:
   (a) Insert all the ciphertexts into a hash table indexed by $N_c$ bits of the non-active S-boxes in the last round.
   (b) For each entry with the same $N_c$ bits value, check whether the input difference is any one of the total $|\Delta_0|$ possible input differences. If a pair satisfies one input difference, then go to the next step.
   (c) For the pairs in each entry, check whether the output differences of active S-boxes in the last round can be caused by the input differences according to the differential distribution table. If the pair passes the test, then go to the next step.
   (d) Guess $n_k$ bits subkeys to decrypt the ciphertext pairs to round $r$ and check whether the obtained output difference at round $r$ is equal to $\Delta_r$. If so, add one to the corresponding counter.
2. Choose the list of the $l$ best key candidates from the counters.
3. Search the list of candidates and all the corresponding master key.

Obviously the time complexity in step 2 is negligible, so we denote $T_a$, $T_b$, $T_c$, $T_d$ and $T_3$ as the time complexity in step (a), (b), (c), (d) and 3, respectively, which are listed in following:

$$\begin{cases} T_a : 2^{N_{st}+N_p} \text{ memory accesses;} \\ T_b : 2^{N_{st}+2N_p-N_c} \text{ memory accesses;} \\ T_c : |\Delta_0| \cdot 2^{N_{st}+N_p-N_c} \text{ memory accesses;} \\ T_d : |\Delta_0| \cdot 2^{N_{st}+N_p-N_c} \cdot p_f \cdot 2^{n_k} \text{ partial decryptions;} \\ T_3 : l \cdot 2^{k-n_k}. \end{cases}$$

This assumes that there are $n_k$ independent subkey bits from the key schedule. In general, $T_d$ can be approximated by $|\varDelta_0| \cdot 2^{N_{st}+N_p-N_c} = T_c$. Since $|\varDelta_0| < 2^{N_p}$, we have $T_c < T_b$. Then the whole time complexity can be expressed as follows:

$$T_a + T_b + T_c + T_d + T_3 \simeq \begin{cases} T_a + T_3 & \text{if } N_p < N_c, \\ T_b + T_3 & \text{if } N_p > N_c, \\ 2T_a + T_3 = 2T_b + T_3 & \text{if } N_p = N_c. \end{cases}$$

If the time complexity in the key searching process $T_3$ is much smaller than the time complexity of the data collection process and the data analysis process, we will take $N_p = N_c$ to minimise the whole time complexity as the minimum value $2T_a$. Otherwise, we can try to take a larger value for $N_p$ to increase the sum of the probabilities for differentials to further reduce the data complexity.

It is worth noting that in the structure attack, any pair of plaintexts with the given input difference is only counted once. In this way, the number of input differences can be increased compared with the condition in Definition 1, improving the efficiency of the attacks. This is especially applicable in an attack scenario where the probability of many differentials are close to $2^{-m}$, implying a low success rate $P_S$. Therefore, a large value for $l$ has to be chosen, which causes the complexity $T_3$ of step 3 to increase. In this case, increasing the number of input differences can help improving the attack, whereas increasing the number of output differences does not have this effect in the case of multiple differential cryptanalysis.

In the case of reduced-round PRESENT, we have the above-mentioned scenario (many differentials with probability close to $2^{-64}$), so that when choosing our set of differentials, we only include a limited number of high-probability differentials to maintain a good success probability $P_S$. For reduced-round Serpent, the probabilities of the differentials are much larger than $2^{-128}$ (the inverse of the block size), so that we can choose more differentials here without affecting the success probability. In order to minimize the time complexity, we choose $N_p = N_c$ according to our model.

### 3.2 Ratio of Weak Keys for Multiple Differentials

In general, the differential probability is related to the value of the key. As we use multiple differentials in the structure attack, we need to consider the ratio of keys which can produce the expected number of right pairs. We call those keys *weak keys* since the attacks are only expected to work for those.

A cipher is called *key-alternating* if it consists of an alternating sequence of unkeyed rounds and simple bitwise key additions. Note that most block cipher proposals, including PRESENT and Serpent, are key-alternating ciphers. The fixed-key cardinality of a differential $N[K](a,b)$ is the number of pairs with input difference $a$ and output difference $b$ where the key $K$ is fixed to a specific value. In [11,10], Daemen and Rijmen give the following theorem.

**Theorem 1.** *Assuming that the set of pairs following a characteristic for a given key can be modeled by a sampling process, the fixed-key cardinality of a differential in a key-alternating cipher is a stochastic variable with the following distribution:*

$$\Pr(N[K](a,b)=i) \approx \text{Poisson}\left(i, 2^{m-1}EDP(a,b)\right),$$

*where $m$ is the block size, $EDP(a,b)$ denotes the expected differential probability of the differential $(a,b)$, and the distribution function measures the probability over all possible values of the key and all possible choices of the key schedule.*

For multiple differentials with multiple input differences and a single output difference, we have $p_j = EDP(a_j,b), 1 \leq j \leq |\Delta_0|$. We denote the fixed-key cardinality of multiple differentials $(a_j,b)$ with a single output difference $b$ by $N[K]\big\{(a_j,b)\big\}_j$. Based on Theorem 1, we can now derive Theorem 2.

**Theorem 2.** *Under the assumptions of Theorem 1, in a key-alternating cipher, the fixed-key cardinality of multiple differentials is a stochastic variable with the following distribution:*

$$\Pr\left(N[K]\big\{(a_j,b)\big\}_j = i\right) \approx \text{Poisson}\left(i, 2^{m-1}\sum_j EDP(a_j,b)\right).$$

*Proof.* The cardinality of multiple differentials equals the sum of the cardinalities of each differential $(a_j,b)$ for the iterative cipher, so we have

$$N[K]\big\{(a_j,b)\big\}_j = \sum_j N[K](a_j,b).$$

From Theorem 1, the cardinality for each differential $(a_j,b)$ has Poisson distribution. Making the standard assumption that the cardinalities of the differentials are independent random variables, the sum still is Poisson distributed with as $\lambda$-parameter the sum of the $\lambda$-parameters of the terms:

$$\lambda = \sum_j 2^{m-1}EDP(a_j,b).$$

□

From Theorem 2, in the structure attack based on the differentials $\Delta_0^i \xrightarrow{r} \Delta_r$, *Probability* $= p_i$, $(1 \leq i \leq |\Delta_0|)$, the ratio of the weak keys $r_w$ that can produce more than or equal to $\mu$ right pairs can be computed as follows:

$$r_w = 1 - \sum_{x=0}^{\mu-1} \text{Poisson}\left(x, 2^{m-1}\sum_{j=1}^{|\Delta_0|} p_i\right).$$

Note that when evaluating the ratio of weak keys, we have a different setting than when dealing with the distribution of the counters in a (multiple) differential attack. While approximating the distribution of the counters with either normal or Poisson distributions was shown to be problematic for accurately estimating the tails [19,4], the distribution of the weak keys instead depends on the *cardinality* of the multiple differentials. In this setting, using the Poisson distribution as in Theorem 2 also yields a good approximation for the tails. This was also experimentally verified with small-scale variants of the block cipher PRESENT [14], with block lengths ranging from 8 to 24 bits.

Additionally, the accuracy of the weak key ratio $r_w$ based on Theorem 2 has been verified by experiments on SmallPresent with a block length of 24 bits, 12 rounds and an master key with 8 bit entropy. 7 differentials with 7 different input and a single output difference were used. It was found that the experimental results very closely follow the theoretical estimate.

## 4 Attack on 18-Round PRESENT

The block cipher PRESENT is designed as a very lightweight cipher. It has a 31-round SPN structure in which the S-box layer has 16 parallel 4-bit S-boxes and the diffusion layer is a bit permutation [7]. The block size is 64 bits and the key size can be 80 bits or 128 bits. One round of PRESENT is illustrated in Fig. 1.

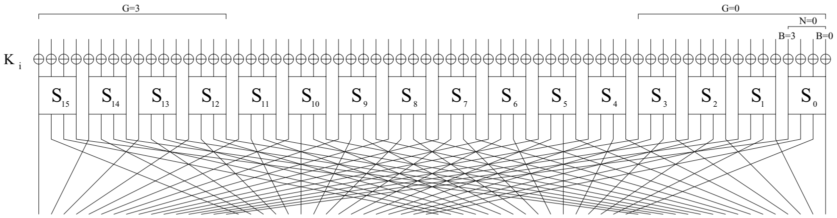

**Fig. 1.** One round of the PRESENT block cipher

PRESENT has been extensively analyzed. Wang presents a differential attack on 16-round PRESENT [20]. Collard *et al.* give a statistical saturation attack for 24-round PRESENT [9]. There are three papers about attacks based on linear hulls for PRESENT [8,17,16], leading to linear attacks for up to 26 rounds. Since the S-box of PRESENT admits linear approximations with single-bit linear masks, the attacker can exploit linear hulls containing many single-bit linear trails over an arbitrary number of rounds. However, for differential attacks, we have to use paths in which two active S-boxes appear per round. Hence, a linear attack will typically be more efficient than differential attacks.

In order to identify a differential with high probability, we must collect more differential paths with high probability for a differential. The differential paths with two active S-boxes in every round have a much bigger contribution to the differential, so we will focus on differential paths with only two active S-boxes in each round. Then we can choose more differentials to improve the attack according to the formulas for the overall time complexity described in Sect. 3, .

### 4.1 Searching Differential Paths for PRESENT

We now give a method to search all differential characteristics with two active S-boxes in each round which have higher probability compared with other differential paths.

First, we introduce some notation. The block size of PRESENT is 64 bits and we can divide 16 nibbles into four groups, in each of which there are four nibbles. We define $G$ as the index of a group, so the four least significant nibbles belong to the group $G = 0$ and the four most significant nibbles belong to the group $G = 3$. Analogously, we denote the index of a nibble in a group as $N$, $N = 0, \ldots, 3$, and $B$ as the $B$-th bit in a nibble, from $B = 0$ to $B = 3$. In this way, the position of any bit can be denoted by a triple $(G, N, B)$, as also illustrated in Fig. 1. The permutation layer $P$ is computed as follows,

$$P(16 \cdot G + 4 \cdot N + B) = 16 \cdot B + 4 \cdot G + N, 0 \leq G, N, B \leq 3.$$

After the permutation layer $P$, the bit $(G, N, B)$ will be transferred to the bit $(B, G, N)$. Here we also give another triple $(G, N, V)$ where $G$ and $N$ are the group index and nibble index, respectively, while $V$ is the difference of the nibble. We wil write $(G_{r,k}, N_{r,k}, B_{r,k})$ for the position of the $k$-th $(k = 1, 2, 3, 4)$ output bit for S-box in round $r$, and $(G_{r,k}, N_{r,k}, V_{r,k})$ for the output difference value of the $k$-th $(k = 1, 2)$ active S-box for nibble $(G_{r,k}, N_{r,k})$ in round $r$.

We focus on finding differential characteristics with two active S-boxes in each round. The foundation for this search is formulated in Theorem 3.

**Theorem 3.** *For the PRESENT block cipher, differential characteristics with only two active S-boxes per round must have the following pattern:*

1. *If two active S-boxes are in the same group in round $r$, their output difference will be equal and must have two non-zero bits to ensure that only two active S-boxes appear in the $(r+2)$-nd round, and two active S-boxes in round $r+1$ will be in the different groups;*
2. *If two active S-boxes are in different groups in round $r$, their output difference will be equal and must have only one non-zero bit to ensure that only two active S-boxes appear in the $(r+1)$-st round, and two active S-boxes in round $r+1$ will be in the same group.*

*Proof.* The output differences for the two active S-boxes are $(G_{r,1}, N_{r,1}, V_{r,1})$ and $(G_{r,2}, N_{r,2}, V_{r,2})$. First, we will prove the case for two active S-boxes in the same group in round $r$. We have $G_{r,1} = G_{r,2}$ and $N_{r,1} \neq N_{r,2}$.

1. $V_{r,1} \in \{1, 2, 4, 8\}$**:** If $V_{r,2} \in \{1, 2, 4, 8\}$, we denote their two non-zero bits as $\{(G_{r,1}, N_{r,1}, B_{r,1}), (G_{r,1}, N_{r,2}, B_{r,2})\}$.
   We have
   $\{(G_{r,1}, N_{r,1}, B_{r,1}), (G_{r,1}, N_{r,2}, B_{r,2})\} \xrightarrow{P} \{(B_{r,1}, G_{r,1}, N_{r,1}), (B_{r,2}, G_{r,1}, N_{r,2})\} \xrightarrow{S}$
   $\{(B_{r,1}, G_{r,1}, N_{r+1,1}), (B_{r,1}, G_{r,1}, N_{r+1,2}), (B_{r,2}, G_{r,1}, N_{r+1,3}), (B_{r,2}, G_{r,1}, N_{r+1,4})\}$
   $\xrightarrow{P} \{(N_{r+1,1}, B_{r,1}, G_{r,1}), (N_{r+1,2}, B_{r,1}, G_{r,1}), (N_{r+1,3}, B_{r,2}, G_{r,1}), (N_{r+1,4}, B_{r,2},$
   $G_{r,1}, )\}$.
   As there are two active S-boxes in round $r+1$, we have $B_{r,1} \neq B_{r,2}$. Because bit $N_{r+1,1}$ and bit $N_{r+1,2}$ are from the same S-box, we have $N_{r+1,1} \neq N_{r+1,2}$.

Similarly, we have $N_{r+1,3} \neq N_{r+1,4}$. There will be four active S-boxes in the $(r+2)$-nd round. If $V_{r,2} \in \{3,5,6,9,10,12\}$, we denote the three non-zero bits as $\{(G_{r,1}, N_{r,1}, B_{r,1}), (G_{r,1}, N_{r,2}, B_{r,2}), (G_{r,1}, N_{r,2}, B_{r,3})\}$.
We have

$$\begin{aligned}&\{(G_{r,1}, N_{r,1}, B_{r,1}), (G_{r,1}, N_{r,2}, B_{r,2}), (G_{r,1}, N_{r,2}, B_{r,3})\}\\ &\xrightarrow{P} \{(B_{r,1}, G_{r,1}, N_{r,1}), (B_{r,2}, G_{r,1}, N_{r,2}), (B_{r,3}, G_{r,1}, N_{r,2}) | B_{r,1} = B_{r,2} \neq B_{r,3}\}\\ &\xrightarrow{S} \{(B_{r,1}, G_{r,1}, N_{r+1,1}), (B_{r,3}, G_{r,1}, N_{r+1,2}), (B_{r,3}, G_{r,1}, N_{r+1,3}) | N_{r+1,2} \neq N_{r+1,3}\}\\ &\xrightarrow{P} \{(N_{r+1,1}, B_{r,1}, G_{r,1}), (N_{r+1,2}, B_{r,3}, G_{r,1}), (N_{r+1,3}, B_{r,3}, G_{r,1})\}.\end{aligned}$$

There will be three active S-boxes in round $r+2$.

2. $V_{r,1} \in \{7,11,13,14,15\}$ **or** $V_{r,2} \in \{7,11,13,14,15\}$**:** There will be at least three active S-boxes in round $r+1$.
3. $V_{r,1}, V_{r,2} \in \{3,5,6,9,10,12\}$**:** We denote the four non-zero bits as $\{(G_{r,1}, N_{r,1}, B_{r,1}), (G_{r,1}, N_{r,1}, B_{r,2}), (G_{r,1}, N_{r,2}, B_{r,3}), (G_{r,1}, N_{r,2}, B_{r,4})\}$.
We have

$$\begin{aligned}&\{(G_{r,1}, N_{r,1}, B_{r,1}), (G_{r,1}, N_{r,1}, B_{r,2}), (G_{r,1}, N_{r,2}, B_{r,3}), (G_{r,1}, N_{r,2}, B_{r,4})\}\\ &\xrightarrow{P} \{(B_{r,1}, G_{r,1}, N_{r,1},)(B_{r,2}, G_{r,1}, N_{r,1}), (B_{r,3}, G_{r,1}, N_{r,2}), (B_{r,4}, G_{r,1}, N_{r,2})\}.\end{aligned}$$

Only if $B_{r,1} = B_{r,3}$ and $B_{r,2} = B_{r,4}$, there will be 2 active S-boxes in round $r+1$, so we have $V_{r,1} = V_{r,2}$. For $B_{r,1} \neq B_{r,2}$, the two active S-boxes in round $r+1$ will be in different groups.

Next, we will prove the case for two active S-boxes in different groups in round $r$. We have $G_{r,1} \neq G_{r,2}$.

1. $V_{r,1} \in \{7,11,13,14,15\}$ **or** $V_{r,2} \in \{7,11,13,14,15\}$**:** There will be at least three active S-boxes in round $r+1$.
2. $V_{r,1} \in \{3,5,6,9,10,12\}$**:** There are at least three non-zero bits, namely $(G_{r,1}, N_{r,1}, B_{r,1}), (G_{r,1}, N_{r,1}, B_{r,2})$ and $(G_{r,2}, N_{r,2}, B_{r,3})$.
We have

$$\begin{aligned}&\{(G_{r,1}, N_{r,1}, B_{r,1}), (G_{r,1}, N_{r,1}, B_{r,2}), (G_{r,2}, N_{r,2}, B_{r,3})\}\\ &\xrightarrow{P} \{(B_{r,1}, G_{r,1}, N_{r,1}), (B_{r,2}, G_{r,1}, N_{r,1}), (B_{r,3}, G_{r,2}, N_{r,2})\}.\end{aligned}$$

For $B_{r,1} \neq B_{r,2}$ and $G_{r,1} \neq G_{r,2}$, there are three active S-boxes in round $r+1$.
3. $V_{r,1} \in \{1,2,4,8\}$**:** From the above proof, we have $V_{r,2} \in \{1,2,4,8\}$. There are two non-zero bits $\{(G_{r,1}, N_{r,1}, B_{r,1}), (G_{r,2}, N_{r,2}, B_{r,2})\}$. We have

$$\begin{aligned}&\{(G_{r,1}, N_{r,1}, B_{r,1}), (G_{r,2}, N_{r,2}, B_{r,2})\} \xrightarrow{P} \{(B_{r,1}, G_{r,1}, N_{r,1}), (B_{r,2}, G_{r,2}, N_{r,2})\}\\ &\xrightarrow{S} \{(B_{r,1}, G_{r,1}, N_{r+1,1}), (B_{r,1}, G_{r,1}, N_{r+1,2}), (B_{r,2}, G_{r,2}, N_{r+1,3}), (B_{r,2}, G_{r,2}, N_{r+1,4})\}\\ &\xrightarrow{P} \{(N_{r+1,1}, B_{r,1}, G_{r,1}), (N_{r+1,2}, B_{r,1}, G_{r,1}), (N_{r+1,3}, B_{r,2}, G_{r,2}), (N_{r+1,4}, B_{r,2}, G_{r,2})\}.\end{aligned}$$

In order to ensure that there are two active S-boxes in round $r+2$, $N_{r+1,1} = N_{r+1,3}$, $N_{r+1,2} = N_{r+1,4}$ and $B_{r,1} = B_{r,2}$. So we have $V_{r,1} = V_{r,2}$ and the two active S-boxes in round $r+1$ are in the same group. □

Based on Theorem 3, a branch-and-bound search algorithm for differential paths can be devised.

Using this algorithm, we search for 16-round differential paths (characteristics) with two active S-boxes in each round having a probability greater than $2^{-92}$. In total, we find 139 *differentials* with probability greater than $2^{-64}$, among

**Table 1.** Filter probability for the structure attack on 18-round PRESENT

| $N_a$ | $(Y_{17,2}, Y_{17,10})$ | $p_f^{(a)}$ |
|---|---|---|
| 2 | $\{(1,1),(1,4),(4,1),(4,4)\}$ | $2^{-24} \cdot (\frac{7}{16})^2 \cdot 4 = 2^{-24.83}$ |
| 3 | $\{(1,9),(1,10),(1,12),(4,9),$ $(4,10),(4,12),(9,1),(9,4),$ $(10,1),(10,4),(12,1),(12,4))\}$ | $2^{-20} \cdot (\frac{7}{16})^3 \cdot 12 = 2^{-19.99}$ |
| 4 | $\{(9,9),(9,10),(9,12),(10,9),$ $(10,10),(10,12),(12,9),(12,10),$ $(12,12),(1,11),(1,13),(4,11),$ $(4,13),(11,1),(11,4),(13,1),(13,4)\}$ | $2^{-16} \cdot (\frac{7}{16})^4 \cdot 17 = 2^{-16.68}$ |
| 5 | $\{(9,11),(9,13),(10,11),(10,13),$ $(12,11),(12,13),(11,9),(11,10),$ $(11,12),(13,9),(13,10),(13,12)\}$ | $2^{-12} \cdot (\frac{7}{16})^5 \cdot 12 = 2^{-14.38}$ |
| 6 | $\{(11,11),(11,13),(13,11),(13,13)\}$ | $2^{-8} \cdot (\frac{7}{16})^6 \cdot 4 = 2^{-13.16}$ |

**Table 2.** Differentials for 16-round PRESENT with $\Delta_{16} = 00000900_x||00000900_x$

| $i$ | $\Delta_0^i$ | $log_2^{p_i}$ | $i$ | $\Delta_0^i$ | $log_2^{p_i}$ |
|---|---|---|---|---|---|
| 1 | $000f0000_x\|\|0000000f_x$ | -62.98 | 10 | $000f0000_x\|\|00000005_x$ | -63.98 |
| 2 | $00070000_x\|\|00000007_x$ | -63.42 | 11 | $000f0000_x\|\|0000000b_x$ | -63.98 |
| 3 | $0f000000_x\|\|00000f00_x$ | -63.68 | 12 | $000f0000_x\|\|0000000d_x$ | -63.98 |
| 4 | $000f0000_x\|\|00000007_x$ | -63.69 | 13 | $00030000_x\|\|0000000f_x$ | -63.98 |
| 5 | $00070000_x\|\|0000000f_x$ | -63.69 | 14 | $00050000_x\|\|0000000f_x$ | -63.98 |
| 6 | $000d0000_x\|\|0000000d_x$ | -63.72 | 15 | $000b0000_x\|\|0000000f_x$ | -63.98 |
| 7 | $00f00000_x\|\|000000f0_x$ | -63.92 | 16 | $000d0000_x\|\|0000000f_x$ | -63.98 |
| 8 | $00090000_x\|\|00000009_x$ | -63.94 | 17 | $f0000000_x\|\|0000000f_x$ | -63.98 |
| 9 | $000f0000_x\|\|00000003_x$ | -63.98 | 18 | $000f0000_x\|\|0000f000_x$ | -63.98 |

which 91 differentials have output difference $\Delta_{16} = 00000500_x||00000500_x$ and 18 differentials have output difference $\Delta_{16} = 00000900_x||00000900_x$. We list them in Table 3 and Table 2, respectively. The differentials have been ordered according to their probabilities in these two tables. In both Table 3 and Table 2, the first column $i$ contains the number of the differential, $\Delta_0^i$ is the input difference and $p_i$ is the probability for each differential. Moreover, we present the number of differential paths ordered by probability for Table 3 in Table 4 and Table 5. In Table 4, the first column denotes the index number in the first column of Table 3. For example, the differentials with number 19 and 20 consist of differential trails with the same probabilities. Columns $2, 3, \ldots, 12$ denote the number of differential paths with probability $2^{-71}, 2^{-73}, \ldots, 2^{-91}$, respectively. In Table 5, the first column denotes the index number in the first column of Table 3. Column $2, 3, \ldots, 13$ denote the number of differential paths with probability $2^{-70}, 2^{-72}, \ldots, 2^{-92}$, respectively. There is no differential path with probability greater than $2^{-70}$ or less than $2^{-92}$ for the 91 differentials.

**Table 3.** Differentials for 16-round PRESENT with output difference $00000500_x||00000500_x$

| $i$ | $\Delta_0^i$ | $log_2^{p_i}$ |
|---|---|---|
| 1 | $000f0000_x\|\|0000000f_x$ | -62.13 |
| 2 | $00070000_x\|\|00000007_x$ | -62.57 |
| 3 | $0f000000_x\|\|00000f00_x$ | -62.79 |
| 4 | $000f0000_x\|\|00000007_x$ | -62.84 |
| 5 | $00070000_x\|\|0000000f_x$ | -62.84 |
| 6 | $000d0000_x\|\|0000000d_x$ | -62.88 |
| 7 | $00f00000_x\|\|000000f0_x$ | -62.95 |
| 8 | $00090000_x\|\|00000009_x$ | -63.10 |
| 9 | $000f0000_x\|\|00000003_x$ | -63.13 |
| 10 | $000f0000_x\|\|00000005_x$ | -63.13 |
| 11 | $000f0000_x\|\|0000000b_x$ | -63.13 |
| 12 | $000f0000_x\|\|0000000d_x$ | -63.13 |
| 13 | $00030000_x\|\|0000000f_x$ | -63.13 |
| 14 | $00050000_x\|\|0000000f_x$ | -63.13 |
| 15 | $000b0000_x\|\|0000000f_x$ | -63.13 |
| 16 | $000d0000_x\|\|0000000f_x$ | -63.13 |
| 17 | $f0000000_x\|\|0000000f_x$ | -63.13 |
| 18 | $000f0000_x\|\|0000f000_x$ | -63.13 |
| 19 | $000d0000_x\|\|00000007_x$ | -63.19 |
| 20 | $00070000_x\|\|0000000d_x$ | -63.19 |
| 21 | $0f000000_x\|\|000000f0_x$ | -63.21 |
| 22 | $00f00000_x\|\|00000f00_x$ | -63.21 |
| 23 | $00000000_x\|\|000f000f_x$ | -63.21 |
| 24 | $0000000f_x\|\|0000000f_x$ | -63.21 |
| 25 | $07000000_x\|\|00000700_x$ | -63.23 |
| 26 | $00700000_x\|\|00000070_x$ | -63.39 |
| 27 | $000b0000_x\|\|0000000b_x$ | -63.44 |
| 28 | $000f0000_x\|\|00000009_x$ | -63.50 |
| 29 | $00090000_x\|\|0000000f_x$ | -63.50 |
| 30 | $0f000000_x\|\|00000700_x$ | -63.50 |
| 31 | $07000000_x\|\|00000f00_x$ | -63.50 |
| 32 | $000b0000_x\|\|00000007_x$ | -63.52 |
| 33 | $00070000_x\|\|0000000b_x$ | -63.52 |
| 34 | $0d000000_x\|\|00000d00_x$ | -63.54 |
| 35 | $70000000_x\|\|00000007_x$ | -63.57 |
| 36 | $00070000_x\|\|00007000_x$ | -63.57 |
| 37 | $000d0000_x\|\|00000009_x$ | -63.58 |
| 38 | $00090000_x\|\|0000000d_x$ | -63.58 |
| 39 | $00000000_x\|\|00070007_x$ | -63.64 |
| 40 | $00000007_x\|\|00000007_x$ | -63.64 |
| 41 | $07000000_x\|\|00000070_x$ | -63.65 |
| 42 | $00700000_x\|\|00000700_x$ | -63.65 |
| 43 | $00700000_x\|\|000000f0_x$ | -63.66 |
| 44 | $00f00000_x\|\|00000070_x$ | -63.66 |
| 45 | $00d00000_x\|\|000000d0_x$ | -63.70 |
| 46 | $09000000_x\|\|00000900_x$ | -63.76 |
| 47 | $000f0000_x\|\|00000f00_x$ | -63.79 |
| 48 | $0f000000_x\|\|0000000f_x$ | -63.79 |
| 49 | $0f000000_x\|\|00000d00_x$ | -63.79 |
| 50 | $0f000000_x\|\|00000b00_x$ | -63.79 |
| 51 | $0f000000_x\|\|00000300_x$ | -63.79 |
| 52 | $0f000000_x\|\|00000500_x$ | -63.79 |
| 53 | $03000000_x\|\|00000f00_x$ | -63.79 |
| 54 | $05000000_x\|\|00000f00_x$ | -63.79 |
| 55 | $0d000000_x\|\|00000f00_x$ | -63.79 |
| 56 | $0b000000_x\|\|00000f00_x$ | -63.79 |
| 57 | $00070000_x\|\|00000003_x$ | -63.84 |
| 58 | $00070000_x\|\|00000005_x$ | -63.84 |
| 59 | $00030000_x\|\|00000007_x$ | -63.84 |
| 60 | $00050000_x\|\|00000007_x$ | -63.84 |
| 61 | $f0000000_x\|\|00000007_x$ | -63.84 |
| 62 | $70000000_x\|\|0000000f_x$ | -63.84 |
| 63 | $000f0000_x\|\|00007000_x$ | -63.84 |
| 64 | $00070000_x\|\|0000f000_x$ | -63.84 |
| 65 | $0d000000_x\|\|00000700_x$ | -63.85 |
| 66 | $07000000_x\|\|00000d00_x$ | -63.85 |
| 67 | $00000f00_x\|\|00000f00_x$ | -63.87 |
| 68 | $00000000_x\|\|0f000f00_x$ | -63.87 |
| 69 | $d0000000_x\|\|0000000d_x$ | -63.88 |
| 70 | $000d0000_x\|\|0000d000_x$ | -63.88 |
| 71 | $00000000_x\|\|000f0007_x$ | -63.91 |
| 72 | $00000000_x\|\|0007000f_x$ | -63.91 |
| 73 | $0000000f_x\|\|00000007_x$ | -63.91 |
| 74 | $00000007_x\|\|0000000f_x$ | -63.91 |
| 75 | $00900000_x\|\|00000090_x$ | -63.92 |
| 76 | $0f000000_x\|\|00000070_x$ | -63.92 |
| 77 | $07000000_x\|\|000000f0_x$ | -63.92 |
| 78 | $00f00000_x\|\|00000700_x$ | -63.92 |
| 79 | $00700000_x\|\|00000f00_x$ | -63.92 |
| 80 | $00f00000_x\|\|00000030_x$ | -63.95 |
| 81 | $00f00000_x\|\|00000050_x$ | -63.95 |
| 82 | $00f00000_x\|\|000000b0_x$ | -63.95 |
| 83 | $00f00000_x\|\|000000d0_x$ | -63.95 |
| 84 | $00300000_x\|\|000000f0_x$ | -63.95 |
| 85 | $00500000_x\|\|000000f0_x$ | -63.95 |
| 86 | $00b00000_x\|\|000000f0_x$ | -63.95 |
| 87 | $00d00000_x\|\|000000f0_x$ | -63.95 |
| 88 | $0d000000_x\|\|000000d0_x$ | -63.95 |
| 89 | $00d00000_x\|\|00000d00_x$ | -63.95 |
| 90 | $00000000_x\|\|000d000d_x$ | -63.95 |
| 91 | $0000000d_x\|\|0000000d_x$ | -63.95 |

**Table 4.** Number of differential paths for differentials in Table 3 (first part)

| $i$ | $2^{-71}$ | $2^{-73}$ | $2^{-75}$ | $2^{-77}$ | $2^{-79}$ | $2^{-81}$ | $2^{-83}$ | $2^{-85}$ | $2^{-87}$ | $2^{-89}$ | $2^{-91}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 9,10,...,18 | 12 | 160 | 986 | 3744 | 9654 | 17440 | 21988 | 18536 | 9280 | 1920 | 0 |
| 19,20 | 12 | 157 | 952 | 3567 | 9092 | 16264 | 20348 | 17068 | 8520 | 1760 | 0 |
| 32,33 | 9 | 123 | 769 | 2913 | 7350 | 12692 | 14780 | 10980 | 4600 | 800 | 0 |
| 35,36 | 9 | 117 | 707 | 2669 | 7056 | 13858 | 20936 | 24568 | 21248 | 11520 | 2560 |
| 37,38 | 6 | 89 | 628 | 2795 | 8562 | 18504 | 27976 | 28004 | 16200 | 3680 | 0 |
| 47,48 | 8 | 104 | 628 | 2348 | 5976 | 10676 | 13340 | 11160 | 5568 | 1152 | 0 |
| 49,50,...,56 | 4 | 64 | 486 | 2336 | 7838 | 19064 | 33976 | 43600 | 38368 | 20736 | 4608 |
| 57,58,...,64 | 9 | 114 | 655 | 2258 | 5092 | 7600 | 7180 | 3800 | 800 | 0 | 0 |
| 65,66 | 4 | 63 | 472 | 2243 | 7448 | 17942 | 31704 | 40376 | 35344 | 19040 | 4224 |
| 69,70 | 3 | 55 | 457 | 2295 | 7744 | 18318 | 30608 | 35268 | 26256 | 11040 | 1920 |
| 80,81,...,87 | 4 | 60 | 438 | 2066 | 6886 | 16766 | 30064 | 38908 | 34584 | 18880 | 4224 |

**Table 5.** Number of differential paths for differentials in Table 3 (second part)

| $i$ | $2^{-70}$ | $2^{-72}$ | $2^{-74}$ | $2^{-76}$ | $2^{-78}$ | $2^{-80}$ | $2^{-82}$ | $2^{-84}$ | $2^{-86}$ | $2^{-88}$ | $2^{-90}$ | $2^{-92}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 12 | 160 | 986 | 3744 | 9654 | 17440 | 21988 | 18536 | 9280 | 1920 | 0 | 0 |
| 2 | 9 | 117 | 707 | 2669 | 7056 | 13858 | 20936 | 24568 | 21248 | 11520 | 2560 | 0 |
| 3 | 4 | 64 | 486 | 2336 | 7838 | 19064 | 33976 | 43600 | 38368 | 20736 | 4608 | 0 |
| 4,5 | 9 | 114 | 655 | 2258 | 5092 | 7600 | 7180 | 3800 | 800 | 0 | 0 | 0 |
| 6 | 3 | 55 | 457 | 2295 | 7744 | 18318 | 30608 | 35256 | 26256 | 11040 | 1920 | 0 |
| 7 | 4 | 60 | 438 | 2066 | 6886 | 16766 | 30064 | 38908 | 34584 | 18880 | 4224 | 0 |
| 8 | 3 | 49 | 383 | 1897 | 6526 | 16098 | 28564 | 35504 | 28928 | 13440 | 2560 | 0 |
| 21,22 | 4 | 56 | 382 | 1708 | 5490 | 13088 | 23300 | 30260 | 27208 | 15168 | 3456 | 0 |
| 23,24 | 0 | 48 | 472 | 2112 | 5724 | 10404 | 13104 | 11336 | 6400 | 1920 | 0 | 0 |
| 25 | 3 | 47 | 351 | 1673 | 5650 | 14212 | 27472 | 41472 | 48928 | 43520 | 25600 | 6144 |
| 26 | 3 | 44 | 316 | 1480 | 4971 | 12516 | 24286 | 36824 | 43656 | 39168 | 23296 | 5632 |
| 27 | 0 | 21 | 274 | 1641 | 6002 | 14746 | 25040 | 29168 | 22336 | 10080 | 1920 | 0 |
| 28,29,30,31 | 3 | 46 | 331 | 1486 | 4562 | 9840 | 14808 | 14736 | 8480 | 1920 | 0 | 0 |
| 34 | 1 | 21 | 205 | 1243 | 5222 | 15940 | 35960 | 59616 | 70464 | 55488 | 24960 | 4608 |
| 39,40 | 0 | 36 | 342 | 1496 | 4090 | 8128 | 12572 | 14936 | 12928 | 7680 | 2560 | 0 |
| 41,42 | 3 | 41 | 275 | 1223 | 3976 | 9836 | 18950 | 28680 | 34008 | 30720 | 18688 | 4608 |
| 43,44 | 3 | 43 | 297 | 1309 | 4000 | 8664 | 13168 | 13268 | 7720 | 1760 | 0 | 0 |
| 45 | 1 | 20 | 188 | 1112 | 4609 | 14004 | 31658 | 52832 | 63048 | 50160 | 22752 | 4224 |
| 46 | 1 | 19 | 175 | 1037 | 4364 | 13596 | 31832 | 55600 | 70336 | 60416 | 30208 | 6144 |
| 67,68 | 0 | 16 | 200 | 1184 | 4420 | 11276 | 20280 | 26080 | 23392 | 13824 | 4608 | 0 |
| 71,72,73,74 | 0 | 36 | 330 | 1330 | 3072 | 4480 | 4280 | 2600 | 800 | 0 | 0 | 0 |
| 75 | 1 | 18 | 160 | 928 | 3857 | 11954 | 28014 | 49196 | 62800 | 54528 | 27520 | 5632 |
| 76,77,78,79 | 3 | 40 | 257 | 1070 | 3152 | 6706 | 10188 | 10412 | 6200 | 1440 | 0 | 0 |
| 88,89 | 1 | 19 | 169 | 949 | 3768 | 11100 | 24650 | 40920 | 49128 | 39696 | 18336 | 3456 |
| 90,91 | 0 | 12 | 178 | 1160 | 4430 | 10944 | 18260 | 20952 | 16416 | 8160 | 1920 | 0 |

### 4.2 Key Recovery Attack on 18-Round PRESENT-80

In this section, we show how to use the 16-round differentials listed in Table 3 to attack 18-round PRESENT-80. The first step is to choose the set of differentials. From the output difference $00000500_x||00000500_x$ at round 16, we can derive that the number of recovered subkey bits in round 17 and round 18 is $8 + 32 = 40$. Those 40 subkey bits are independent according to the key schedule. In this attack, we will use the whole codebook and set the size of the candidates of subkey counters $l$ to $2^{36}$. In our structure attack, we will use Blondeau *et al.*'s method (see Sect. 2) to compute the success rate. With Equation (1), we have $n_k = 40$, $l = 2^{36}$ and $N = 2^{64}$. We gradually increase the number of differentials with higher probability from Table 3 to compute the success probability for every case. As a result, we found that the success rate will increases as $|\Delta_0| = i$ increases if $1 \leq i \leq 36$. The success probability is 85.95% as $|\Delta_0| = 36$. If we add the $i$-th $(37 \leq i \leq 91)$ differential to the set, the success probability will be reduced. This implies that the $i$-th $(37 \leq i \leq 91)$ differential has no contribution to reduce the data complexity since its probability is too low. Therefore, in our attack, we will only use the first 36 differentials in Table 3.

If we use multiple differentials cryptanalysis for PRESENT following Blondeau *et al.*, we can choose more output difference values. We can add the 18 differentials in Table 2 to the set of 36 differentials. The input difference values for the 18 differentials belong to the set of the input difference values for the 36 differentials, so we have $|\Delta_0| = 36$ and $|\Delta_{16}| = 2$. Then we get $p_* = 2^{-62.74}$ and $p = 2^{-63}$. As $\tau$ $(p < \tau < p_*)$ increases, $G(\tau, p)$ will decrease. Even if we take $\tau = p_*$, $G(\tau, p)$ is still larger than $(1 - \frac{l-1}{2^{n_k}-2})$, so the attack will not work for $l = 2^{36}$. Therefore, our structure attack works better for PRESENT than the multiple differential cryptanalysis presented in [4].

Moreover, we have identified the differential trails with two active S-boxes per round but more than two active S-boxes in the last round. As a result, those differentials have no advantage compared with the differentials in Table 3. Therefore, these differentials do not contribute to improving multiple differential cryptanalysis for PRESENT.

We will use the structure attack for 18-round PRESENT-80 with the first 36 differentials with $p_* = 2^{-63.14}$ and $p = 2^{-64}$. For the 36 input differences, there are 10 active S-boxes in the first round which are nibbles 0, 1, 2, 3, 4, 8, 12, 13, 14 and 15, so the S-boxes for the nibbles 5, 6, 7, 9, 10 and 11 are all non-active.

We construct $2^{24}$ structures of $2^{40}$ chosen plaintexts each. In each structure, all the inputs to the 6 non-active S-boxes in the first round take a fixed random value, while 40 bits of input to 10 active S-boxes take $2^{40}$ possible values. In all structures, there are $2^{24} \cdot 2^{39} = 2^{63}$ pairs for each possible differential. The sum of the probabilities for all 36 differentials is $2^{-57.97}$, so the number of right pairs is $2^{63} \cdot 2^{-57.97} = 2^{5.03}$.

According to the output difference of 16-round differentials, there are two active S-boxes in round 17 in nibble 2 and 10 whose input difference is 5 and the possible output differences will be 1, 4, 9, 10, 11, 12 or 13. After the bit permutation, 8 output bits from the two active S-boxes in round 17 will be one input bit to 8 different S-boxes in round 18 respectively. As the number of non-zero bits among the 8 output bits is at most 6, the maximum number of active S-boxes for round 18 is 6 and the minimum number of active S-boxes for round 18 is 2. We denote the number of active S-boxes in round 18 as $N_a$ $(2 \leq N_a \leq 6)$, the output difference for the $j$-th S-box in round $i$ as $Y_{i,j}$, the filter probability with $N_a$ active S-boxes in round 18 as $p_f^{(a)}$. We present the filter probability for different values of $N_a$ in Table 1. The filter probability for the ciphertext pairs $\beta$ according to active S-boxes can be computed with the sum of column 3 in Table 1, and we get $\beta = 2^{-12.55}$.

We now describe in detail the attack procedure of Sect. 3 for 18-round PRESENT-80. We have $|\Delta_0| = 36$, $\sum_{i=1}^{|\Delta_0|} p_i = 2^{-57.97}$, $N_{st} = 24$, $N_p = 40$, $N_c = 32$, $\beta = 2^{-12.55}$, $p_f = 2^{-44.55}$, $n_k = 40$ and $l = 2^{36}$. We denote $T_a$, $T_b$, $T_c$, $T_d$ and $T_3$ as the time complexity in step (a), (b), (c) (d) and 3, respectively, which are as follows: $T_a = 2^{64}$ memory accesses, $T_b = 2^{72}$ memory accesses, $T_c = 36 \cdot 2^{32}$ memory accesses, $T_d = 36 \cdot 2^{31} \cdot 2^{-12.55} \cdot 2^{40} \cdot (\frac{1}{2} + \frac{1}{8}) \cdot 2 = 2^{65.20}$ 1-round encryptions and $T_3 = 2^{36} \cdot 2^{40} = 2^{76}$ 18-round encryptions. Therefore, the total time complexity will be $2^{76}$ 18-round encryptions. The data complexity is $2^{64}$ chosen plaintexts and the memory requirements are $2^{40}$ 128-bit cells for the hash table, which can be reused for the $2^{40}$ counters. The success probability is 85.95%.

The ratio of weak key satisfying the sum of the probabilities of the 36 differentials is computed as follows:

$$r_w = 1 - \sum_{x=0}^{\mu-1} \text{Poisson}\left(x, 2^{n-1} \sum_{j=1}^{N_d} p_i\right) = 1 - \sum_{x=0}^{2^{5.03}-1} \text{Poisson}\left(x, 2^{63} \cdot 2^{-57.97}\right) = 0.57.$$

This means that the number of weak keys for which our attack can succeed is $2^{80} \cdot 0.57 = 2^{79.19}$ for PRESENT-80. A comparison with the attack of [6] can be found in Section 2.

## 5 Attack on Reduced-Round Serpent

Serpent was one of the five AES candidates in the final round; it is an SPN block cipher with 32 rounds [1]. In our attacks, we consider Serpent from rounds 4 to 11.

In the previous differential cryptanalysis of Serpent in [3], Biham *et al.* used the structure attack for Serpent. They identify a differential characteristic for $\frac{1}{2} + 5$ rounds staring from the linear transformation with fewer active S-boxes (13 active S-boxes) in the first half round, then extend it backwards to 6 rounds. Moreover, there is only one differential characteristic in each differential due to the strong avalanche characteristics of Serpent. Biham *et al.* claim that $2^{14}$ differential characteristics with probability $2^{-93}$ have been found. However, it can be shown that there are only $2^{13}$ differential characteristics with probability $2^{-93}$. The proof has been omitted due to space constraints.

For the differential characteristics, the output difference of S-boxes in the first round is $\{0906b010_x||00000080_x||13000226_x||06040030_x\}$. We will use all the possible non-zero input differences according to the output differences for the S-boxes ($S_4$) in the first round. According to the differential distribution table of $S_4$, we have $|\varDelta_0| = 2^{35.32}$ and $\sum_{i=1}^{|\varDelta_0|} p_i = 2^{-65}$ which is equal to the probability of the differential characteristic from round 2 to round 6.

We now apply the structure attack described in Sect. 3. We construct $2^{19}$ structures of $2^{52}$ chosen plaintexts each. In each structure, all the inputs to non-active S-boxes in the first round are fixed to some random value, while the 52 bits of input to all the active S-boxes take all the $2^{52}$ possible values. There are $2^{19} \cdot 2^{51} = 2^{70}$ pairs for each differential characteristic. We expect that about $2^{70} \cdot 2^{-65} = 2^5$ pairs produce the output difference $\varDelta_6$. In order to reduce the time complexity and ensure a higher success probability, 52 bits subkey are guessed after the data collection process. After retrieving 52 bits of the subkey, we can use the right pairs to recover the remaining 24 bits of the subkey.

The success probability $P_S$ can be computed with Equation (1). Here $N = 2^{71}$, $|\varDelta_0| = 2^{35.32}$, $p_* = 2^{-65} \cdot 2^{-35.32} \cdot 2^{52} = 2^{-48.32}$, $N_s = 2^{70} \cdot 2^{35.32} \cdot 2^{-52} = 2^{53.32}$, $p = 2^{-52}$, $n_k = 52$, $l = 2$, $\beta = 2^{-26.22}$, hence we get $P_S = 89.87\%$.

The time complexity is $2^{27.10} \cdot 2^{52} \cdot 13/32 = 2^{77.81}$ one-round encryptions which is equivalent to $2^{74.99}$ 7-round encryptions, the data complexity is $2^{71}$ chosen plaintexts and the memory requirements are $2^{52}$ hash cells of 256 bits and $2^{52}$ 32-bit counters storing $2^5$ pairs each, hence using about $2^{57}$ 256-bit words. This attack consequently applies to Serpent with all key sizes of 128,192 and 256 bits.

The attack can be further extended to 8-round Serpent-256. By exhaustively searching the 128-bit subkey in the last round to decrypt to round 7, the above attack for 7 rounds can be applied. The time complexity is $2^{203.81}$ 8-round encryptions, the data complexity is $2^{71}$ chosen plaintexts and the memory requirements are the same as for the 7-round attack. This attack therefore applies only to Serpent with a 256-bit key.

In comparison, the previous differential attack for 7-round Serpent described in [3] has a time complexity of $2^{85}$ memory accesses and a data complexity of $2^{84}$ chosen plaintexts. For the previous differential attack on 8-round Serpent, the time complexity is $2^{213}$ memory accesses and the data complexity is $2^{84}$ chosen plaintexts. This implies that our attacks require much less chosen plaintexts and improve the time complexity.

It is possible to further reduce the data requirements at the expense of the time complexity. We have identified another set of differentials for 5.5 rounds which have 16 instead of 13 active S-boxes in the first round (the sequence of active S-Boxes is 16–10–6–2–1–5, and there are $2^{41.49}$ input differences). The combined probability of these differentials is $2^{-62.85}$, leading to a total time complexity greater than the previously described attack.

The ratio of weak keys satisfying the probability of the multiple differentials is computed as follows:

$$r_w = 1 - \sum_{x=0}^{\mu-1} \text{Poisson}\left(x, 2^{n-1}\sum_{j=1}^{N_d} p_i\right) = 1 - \sum_{x=0}^{2^5-1} \text{Poisson}\left(x, 2^{70}\cdot 2^{-65}\right) = 0.52.$$

This means that this attack is expected to work with about half of all possible keys, independent of the key size.

## 6 Conclusion

In this paper, we give a general model for the structure attack, providing guidance on how to choose the set of differentials to minimize the time complexity. As concrete applications of our model, we present structure attacks on 18-round PRESENT and improve the previous differential cryptanalytic results for the Serpent block cipher. To the best of our knowledge, those attacks are the best known differential attacks on these two block ciphers.

Comparing our model for structure attacks against the general model for multiple differential cryptanalysis proposed in [4], we conclude that the limitation for the set of input differences imposed by the model of [4] excludes many valuable differentials. We show that in structure attacks, a very important – and often particularly efficient – subclass of multiple differential attacks, this restriction can be relaxed. In our model presented in Sect. 3, the analysis of an attack can be carried out without this assumption.

The relevance of the limitation imposed by the condition of Definition 1 is additionally supported by our concrete application of the structure attack to PRESENT, which is more efficient than the multiple differential cryptanalysis with different output differences described in [4] and [6] where this condition was necessary. By removing this limitation, we have identified new sets of differentials that improve on the previous analysis.

It remains an interesting open question to find a block cipher other than PRESENT for which multiple differential cryptanalysis with multiple output differences produces superior results to the structure attack. Furthermore, our attack model can be used as a guidance to improve differential attacks for other algorithms. Applying it to other block ciphers than PRESENT or Serpent will be subject of future work.

**Acknowledgements.** We would like to thank Vincent Rijmen for valuable advice and Kerem Varici for his support for the work on PRESENT. The work in this paper was supported in part by the European Commission through the ICT programme under contract ICT-2007-216676 ECRYPT II and in part by the Concerted Research Action (GOA) TENSE 2011 of the Flemish Government, the IAP Program P6/26 BCRYPT of the Belgian State (Belgian Science Policy) and by the Research Fund KU Leuven (project OT/08/027).

## References

1. Anderson, R., Biham, E., Knudsen, L.R.: A Proposal for the Advanced Encryption Standard. NIST AES proposal (1998)
2. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology 4(1), 3–72 (1991)
3. Biham, E., Dunkelman, O., Keller, N.: The Rectangle Attack - Rectangling the Serpent. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 340–357. Springer, Heidelberg (2001)
4. Blondeau, C., Gérard, B.: Multiple Differential Cryptanalysis: Theory and Practice. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 35–54. Springer, Heidelberg (2011)
5. Blondeau, C., Gérard, B.: Private communication: The 561 Differentials (2011)
6. Blondeau, C., Gérard, B.: Multiple Differential Cryptanalysis: Theory and Practice (Corrected). Cryptology ePrint Archive: Report 2011/115
7. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)
8. Cho, J.: Linear Cryptanalysis of Reduced-Round PRESENT. In: Pieprzyk, J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 302–317. Springer, Heidelberg (2010)
9. Collard, B., Standaert, F.-X.: A Statistical Saturation Attack against the Block Cipher PRESENT. In: Fischlin, M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 195–210. Springer, Heidelberg (2009)
10. Daemen, J., Rijmen, V.: Probability distributions of correlations and differentials in block ciphers. Journal of Mathematical Cryptology 1(3), 221–242 (2007)
11. Daemen, J., Rijmen, V.: Probability distributions of Correlation and Differentials in Block Ciphers (2005), http://eprint.iacr.org/2005/212
12. Dunkelman, O., Indesteege, S., Keller, N.: A Differential-Linear Attack on 12-Round Serpent. In: Chowdhury, D.R., Rijmen, V., Das, A. (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 308–321. Springer, Heidelberg (2008)
13. Lai, X., Massey, J.L.: Markov Ciphers and Differential Cryptanalysis. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 17–38. Springer, Heidelberg (1991)
14. Leander, G.: Small scale variants of the block cipher PRESENT. Cryptology ePrint Archive, Report 2010/143 (2010)
15. Matsui, M., Nakajima, J.: On the Power of Bitslice Implementation on Intel Core2 Processor. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 121–134. Springer, Heidelberg (2007)
16. Nakahara Jr., J., Sepehrdad, P., Zhang, B., Wang, M.: Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT. In: Garay, J.A., Miyaji, A., Otsuka, A. (eds.) CANS 2009. LNCS, vol. 5888, pp. 58–75. Springer, Heidelberg (2009)
17. Ohkuma, K.: Weak Keys of Reduced-Round PRESENT for Linear Cryptanalysis. In: Jacobson Jr., M.J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2009. LNCS, vol. 5867, pp. 249–265. Springer, Heidelberg (2009)
18. Selçuk, A.A., Biçak, A.: On Probability of Success in Linear and Differential Cryptanalysis. In: Cimato, S., Galdi, C., Persiano, G. (eds.) SCN 2002. LNCS, vol. 2576, pp. 174–185. Springer, Heidelberg (2003)
19. Selçuk, A.A.: On Probability of Success in Linear and Differential Cryptanalysis. Journal of Cryptology 21(1), 131–147 (2008)
20. Wang, M.: Differential Cryptanalysis of Reduced-Round PRESENT. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 40–49. Springer, Heidelberg (2008)