The Notion of Transparency Order, Revisited

Huizhong Li, Yongbin Zhou, Jingdian Ming, Guang Yang, Chengbin Jin

China State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing, China, 100093
School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China, 100049
{*lihuizhong,zhouyongbin,mingjingdian,yangguang2,jinchengbin*}*@iie.ac.cn*

Abstract. We revisit the definition of Transparency Order (TO) and that of Modified Transparency Order (MTO) as well, which were proposed to measure the resistance of an S-box against Differential Power Analysis (DPA). We spot a definitional flaw in original TO, which is proved to have significantly affected the soundness of TO and hinder it to be a good quantitative security criterion. Regretfully, the flaw itself remains virtually undiscovered in MTO, either. Surprisingly, MTO overlooks this flaw and yet it happens to incur no bad effects on the correctness of its formulation, even though the start point of this formulation is highly questionable. It is also this neglect of the flaw that made MTO take a variant of multi-bit DPA attack into consideration, which was mistakenly thought to appropriately serve as an alternative powerful attack. Based on this observation, we also find that MTO introduces such an alternative adversary that it might overestimate the resistance of an S-box in some cases, as the variant of multi-bit DPA attack considered in MTO is not that powerful as one may think. This implies the soundness of MTO is also more or less arguable. Consequently, we fix this definitional flaw, and provide a revised definition in which a powerful adversary is also involved. For demonstrating validity and soundness of our revised TO (RTO), we adopt both optimal 4×4 S-boxes and 8×8 S-boxes as study cases, and present simulated and practical DPA attacks as well on implementations of those S-boxes. The results of our attacks verify our findings and analysis as well. Furthermore, as a concrete application of the revised TO, we also present the distribution of RTO values for sixteen optimal affine equivalence classes of 4×4 S-boxes. Finally, we give some recommended guidelines on how to select optimal 4×4 S-boxes in practical implementations.

Keywords: Transparency order · Differential power analysis · S-box · Hamming weight leakage model.

1 Introduction

When discussing the security of modern ciphers, it is often natural to discuss their resistance to certain cryptanalytic attacks. Broadly speaking, symmetric ciphers embedded in cryptographic devices are prone to two main kinds of attacks.

The first one is called classical cryptanalytic attacks like linear cryptanalysis [25] and differential cryptanalysis [2], which basically rely on the mathematical properties of those cryptographic primitives involved in cryptosystems. The second one is called Side-Channel Attacks (SCAs), which essentially exploit physical leakages from actual implementations of ciphers. And the efficiency of SCAs is usually higher than the one of classical cryptanalytic attacks in the cases which side-channel leakages can be obtained by adversaries [5]. Since timing attack was introduced by Kocher [20] in the year 1996, SCAs have become an active research area. Besides running time, other typical kinds of physical leakages such as power consumption [19] and electro-magnetic emanations [7] can also be utilized to recover the sensitive data of the underlying cryptosystems. Among those numerous SCA methods, power analysis attacks are one of the most effective methods, of which DPA is a very basic one.

To counteract classical cryptanalytic attacks, Substitution Boxes (S-boxes) used in symmetric ciphers as primitives are often designed to fulfill some cryptographic criteria such as high nonlinearity and high algebraic degree [11]. On the other hand, it is evident that S-boxes could also be the primary target of DPA attacking process, and the side-channel resistance of a cipher component is roughly inversely proportional to the nonlinearity degree of S-boxes [5, 37]. Several studies have shown that with respect to DPA, some S-boxes leak more than others [36, 33], even those S-boxes with identical mathematical properties which are considered in classical cryptanalysis. From the designer's point of view, before using other countermeasures against DPA (e.g., hiding and masking schemes [9, 10, 24]), the S-boxes must be chosen carefully to have high DPA resistance in addition to good resistance to classical cryptanalytic attacks. Therefore, how to measure the intrinsic resistance of S-boxes against DPA is an important issue.

Regarding the resistance of S-boxes against DPA, there are three metrics so far, namely the DPA signal-to-noise ratio (SNR), (Modified) Transparency Order and confusion coefficient. SNR was first proposed to measure the level of leakages expected from an S-box design, which is highly correlated with the implementation and device of the cryptosystem [17]. Then, under the assumption of Hamming weight leakage model, Prouff introduced the notion of transparency order (TO) [37], which quantifies the basic DPA resilience from mathematical properties of the S-box itself. In 2012, Fei et al. presented confusion coefficients to evaluate the SCA success rate of a cryptographic system [15]. However, the main contribution of this work is to explicitly decouple contributions from physical implementations and cryptographic algorithms on the leakages. For DPA attacks, the confusion coefficient indictor can only quantify the resistance of S-boxes against single-bit DPA. Therefore, if only the S-box property is considered to evaluate the DPA resistance of cryptosystems, the transparency order is the most appropriate metric among the above three metrics.

Interestingly, the notion of TO did not attract much attention in the first few years, even though it was proposed in 2005. Until 2012, there began to be some research works exploring this property and verifying its effectiveness. Generally speaking, TO is mainly used to select optimal S-boxes for cryptographic algo-

rithms. In [27], [28] and [29], Mazumdar et al. constructed a variety of rotation symmetric S-boxes and 8×8 S-boxes with high nonlinearity and DPA resistance in terms of TO property. Picek et al. used genetic algorithms to search Boolean functions [31], 8×8 S-boxes [32] and 4×4 S-boxes [33] with smaller TO values. In addition, Evci et al. and Kavut et al. constructed rotation symmetric S-boxes with lower TO values for 8×8 size [13] and 6×6 size [18], respectively. The above work also confirmed the effectiveness of TO in some scenarios with several implementation results on cryptographic devices such as SASEBO-GII board [28, 29] and ATmega163 smartcard [32, 33]. However, in 2014 Chakraborty et al. showed that the original TO is flawed and consequently they suggested the modified transparency order (MTO) [8] to quantify the resistance of S-boxes against a variant kind of DPA attack [1] in Hamming weight leakage model. The proposal of MTO has an important impact on the study of transparency order. Since then, many researches of constructing or searching for S-boxes with high DPA resistance adopted MTO as a metric, such as the generation of 8×8 S-boxes and 4×4 S-boxes [34, 36], and construction of 8×8 rotation symmetric S-boxes [26].

Our contributions. In this paper, we revisit the notions of TO and MTO. We spot a definitional flaw in the work of TO in addition to limitations pointed out in MTO, which seriously affected the soundness of TO. The work of MTO did not discover this flaw but coincidentally bypass it by applying a less powerful DPA attack. However, the "enhanced" DPA attack considered in MTO is actually not as powerful as the original DPA. Consequently, we argue that, MTO actually overestimates the resistance of S-boxes against DPA attacks in Hamming weight leakage model. On this basis, this work essentially amends TO and MTO, and proposes the notion of revised transparency order (RTO). We verify the soundness of RTO through simulated and practical experiments. Furthermore, this paper studies the distribution of RTO values in sixteen optimal affine equivalence classes of 4×4 S-boxes, and makes some recommendations on how to select optimal 4×4 S-boxes in practical implementations.

The rest of the paper is organized as follows. Notations and preliminaries are reviewed in Section 2. Section 3 revisits the definition of TO and MTO, and points out a flaw in TO and one weakness of MTO respectively. Then we amends TO and MTO, and the definition of revised transparency order (RTO) is proposed in Section 4. In Section 5, we verify the validity and soundness of RTO in combination with simulated and practical experiments. Section 6 shows the distribution of S-boxes with different RTO values in the range of sixteen optimal affine equivalence classes of 4×4 S-boxes and makes some recommended guidelines on the selection of 4×4 S-boxes. Finally, we conclude our work in Section 7.

2 Notations and preliminaries

In this section, we give basic notions about cryptographic properties of S-boxes and necessary information about DPA attacks. In particular, we introduce the notions of transparency order (TO) and modified transparency order (MTO).

2.1 Boolean functions and S-boxes

Let $\mathbb{F}_2^n$ be the vector space that contains all the n-bit binary vectors, where n is a positive integer. For every vector $u \in \mathbb{F}_2^n$, we denote by $\mathsf{H}(u)$ the *Hamming weight* of u. A Boolean function on n variables can be viewed as a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, and the mappings from the vector space $\mathbb{F}_2^n$ to the vector space $\mathbb{F}_2^m$ are called (n, m)-vectorial Boolean functions where $m \leqslant n$. An (n, m)-function F is said to be balanced if every element $y \in \mathbb{F}_2^m$ admits the same number 2^{n-m} of pre-images by F. Such a function F that satisfies cryptographic properties like resisting linear and differential cryptanalysis is called an $n \times m$ S-box.

The inner product of each pair of vectors $x = \{x_1, \ldots, x_n\}$ and $u = \{u_1, \ldots, u_n\}$ both belonging to $\mathbb{F}_2^n$ is defined as $x \cdot u = \bigoplus_{i=0}^{n} x_i u_i$, where $\oplus$ denotes the additions mod 2. The *Walsh transform* of the Boolean function $f(x)$ is an integer valued function over $\mathbb{F}_2^n$ which is defined as $W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus x \cdot u}$ for every $u \in \mathbb{F}_2^n$. The *autocorrelation transform* of the function $f(x)$ with respect to u is defined as $\mathcal{A}_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus u)}$. And the *cross-correlation spectrum* between two Boolean functions f_1, f_2 is defined as the value $\mathcal{C}_{f_1,f_2}(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f_1(x) \oplus f_2(x \oplus u)}$ for every $u \in \mathbb{F}_2^n$ (note that we have $\mathcal{C}_{f,f}(u) = \mathcal{A}_f(u)$). Particularly, we denote $\mathcal{C}_{f_1,f_2}(0)$ as $Cor(f_1, f_2)$. The Walsh and autocorrelation spectra are important properties for quantifying the cryptographic resistance of Boolean functions that be used as cryptographic primitives, and it is generally expected that the maximum absolute value in these two spectra should be low for better resistance against classical cryptanalysis [6].

For each (n, m)-function F, the Boolean functions $f_1, \ldots, f_m$ defined for every $x \in \mathbb{F}_2^n$ by $F(x) = (f_1(x), \ldots, f_m(x))$ are called the coordinate functions of F. The j-th component function of the function F is a single output Boolean function $u \cdot F$, which can be denoted as F_j. For every F_j, we have:

$$F_j = \frac{1}{2} - \frac{1}{2}(-1)^{F_j}, \tag{1}$$

Proposition 1. *An (n, m)-function F is balanced if and only if $W_{F_j}(0)$ equals to zero for every $j \in \{1, \ldots, m\}$.*

2.2 Basics of DPA attacks

DPA performs statistical analysis (calculate the difference of means) to retrieve secret keys from the power consumption of cryptographic devices. It exploits the fact that the power consumption of cryptographic devices is dependent on the activity of devices and in particular is dependent on the value of temporary

variables in cryptographic algorithms. Initial results in this direction have been presented by Kocher et al. [19]. The attackers need to measure a sample of power traces $T_{\dot{K}}(x)$ related to a sufficiently large number of public data x (e.g. plaintexts or ciphertexts) and a constant secret key $\dot{K}$. Then a DPA attack can be done by computing a so-called differential trace.

In a *single-bit DPA*, a particular bit of the intermediate value is considered. The attackers partition the power traces in two bins by predicting whether the bit value is zero or one, corresponding to the guessed key K. One usually uses a Boolean function D called selection function to calculate this bit value. For every 3-tuple $(x, K, j) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \times \{1, \ldots, m\}$ which denotes the value of the j^{th} bit of $F(x \oplus K)$, the selection function can be written as $D(x, K, j)$. Let $X(i)$ denote the i^{th} public data, and j denote the index of the targeted bit. $K \in \mathbb{F}_2^n$ and $\dot{K} \in \mathbb{F}_2^n$ denote the guessed key and secret key, respectively. Then the differential trace $\Delta_{K,\dot{K}}(N, j)$ can be calculated by:

$$\Delta_{K,\dot{K}}(N,j) = \frac{\sum_{i=1}^{N} D\left(X(i), K, j\right) T_{\dot{K}}\left(X(i)\right)}{\sum_{i=1}^{N} D\left(X(i), K, j\right)} - \frac{\sum_{i=1}^{N} \left(1 - D\left(X(i), K, j\right)\right) T_{\dot{K}}\left(X(i)\right)}{\sum_{i=1}^{N} \left(1 - D\left(X(i), K, j\right)\right)}, \tag{2}$$

Using Eq. (2), one can calculate a differential trace for each guessed key, and the vector $\Delta_{K,\dot{K}}(N, j)$ should show a peak for the correct key $K = \dot{K}$. For a large value N, the value $\Delta_{K,\dot{K}}(N, j)$ approximately equals to $\Delta_{K,\dot{K}}(2^n, j)$, and the inputs of D loop through $\mathbb{F}_2^n$. To simplify notations, we denote $\Delta_{K,\dot{K}}(2^n, j)$ by $\Delta_{K,\dot{K}}(j)$.

Since the single-bit DPA only utilizes the information of a certain bit of the intermediate value, in order to improve the efficiency of attack, Messerges proposed *multi-bit DPA* to simultaneously consider several bit indices j [30]. The multi-bit DPA attack is done by computing the absolute value of the sum of $\Delta_{K,\dot{K}}(N, j)$ for several indices $j \in \{1, \ldots, m\}$ (all m indices for m-bit intermediate in general) to obtain $\delta_{K,\dot{K}} = |\sum_{j=1}^{m} \Delta_{K,\dot{K}}(N, j)|$. As in the single-bit case, $\delta_{K,\dot{K}}$ is expected to show a peak when $K = \dot{K}$. This attack has been proved to be the most efficient attack in Hamming weight leakage model (with Gaussian noise or not) [12].

In [1], a *variant multi-bit DPA* attack has been proposed to add the absolute values of the $\Delta_{K,\dot{K}}(N, j)$ instead of the values themselves to build $\delta'_{K,\dot{K}} = \sum_{j=1}^{m} |\Delta_{K,\dot{K}}(N, j)|$. This approach might be a valuable alternative of multi-bit DPA in practice such as when the device leaks information in random linear model rather than Hamming weight model [12].

2.3 Transparency order and modified transparency order of S-boxes

2.3.1 Transparency order

As mentioned above, DPA attacks provide attackers several kinds of distinguishers based on differential traces $\Delta_{K,\dot{K}}(N, j)$ to recover the secret key $\dot{K}$. The

distinguishers take the maximum value when hypothesis key is equal to correct key. From the designer's point of view, the smaller the difference between the score of the distinguisher for the correct key and the average score for the other hypotheses, the more difficult it is for attackers to identify the correct secret key. Based on this basic idea, transparency order (TO) [37] was introduced to measure the resistance of S-boxes against multi-bit DPA attack in Hamming weight model. This model assumes that the cryptographic device leaks information in the form of $T_{\dot{K}}(x) = \mathsf{H}(F(x \oplus \dot{K}) \oplus \beta) + \omega$, where x and $\dot{K}$ respectively denote the public data and the secret key, where $\beta \in \mathbb{F}_2^m$ denotes the register initial state which is assumed to be constant, and ω denotes an independent noise. TO not only depends on the S-box's algebraic properties but also depends on the value of β. After derivation based on certain assumptions, the TO property of a $n \times m$ S-box F is defined as follows. The S-box will be more resistant against DPA attacks if it shows a low TO value.

$$\mathrm{TO(F)} = \max_{\beta \in \mathbb{F}_2^{\mathrm{m}}} \left(|\mathrm{m} - 2\mathsf{H}(\beta)| - \frac{1}{2^{2\mathrm{n}} - 2^{\mathrm{n}}} \sum_{\mathrm{a} \in \mathbb{F}_2^{\mathrm{n}*}} \left| \sum_{\mathrm{i}=1}^{\mathrm{m}} (-1)^{\beta_{\mathrm{i}}} \mathcal{A}_{\mathrm{F_i}}(\mathrm{a}) \right| \right) . \quad (3)$$

2.3.2 Modified transparency order

In [8], Chakraborty et al. pointed out that TO is based on the assumption that coordinates of an S-box are uncorrelated with each other, which means that for every $i \neq j$ and every $(K, \dot{K})$, cross-correlation terms $C_{F_i,F_j}(K \oplus \dot{K})$ of an $n \times m$ S-box F can be considered to be zero. The authors explained that this assumption cannot be satisfied in real world S-boxes (such as AES S-box), and then presented the notion of modified transparency order (MTO). Different from TO, MTO quantifies the resistance of S-boxes against the variant multi-bit DPA rather than multi-bit DPA attack in Hamming weight model. This new notion is defined in Eq. (4), and has been shown to be more useful for quantifying the DPA resistance of S-boxes than TO [34].

$$\mathrm{MTO(F)} = \max_{\beta \in \mathbb{F}_2^{\mathrm{m}}} \left(\mathrm{m} - \frac{1}{2^{2\mathrm{n}} - 2^{\mathrm{n}}} \sum_{\mathrm{a} \in \mathbb{F}_2^{\mathrm{n}*}} \sum_{\mathrm{j}=1}^{\mathrm{m}} \left| \sum_{\mathrm{i}=1}^{\mathrm{m}} (-1)^{\beta_{\mathrm{i}} \oplus \beta_{\mathrm{j}}} \mathcal{C}_{\mathrm{F_i},\mathrm{F_j}}(\mathrm{a}) \right| \right) . \quad (4)$$

3 A flaw in TO and one weakness of MTO

In this section, we first revisit TO and point out its definitional flaw in DPA formulation, which significantly affects the soundness of TO. In Section 3.2, by revisiting MTO, we argue that it virtually overlooks this flaw and might overestimate the resistance of S-boxes being exposed to DPA attacks.

3.1 A definitional flaw in TO

As mentioned in Section 2.3.2, Chakraborty et al. have pointed out that the notion of TO is based on a certain unrealistic assumption [16]. Although this

unreasonable assumption is fixed in the work of MTO, another definitional flaw in DPA formulation is still overlooked.

To illustrate this serious flaw in DPA formulation, let us first review the formulation of single-bit DPA. Assuming the leakage model of device is Hamming distance model, for every pair $(x, \dot{K})$, the power consumption $T_{\dot{K}}(x)$ in Eq. (2) satisfies the relation $T_{\dot{K}}(x) = \mathsf{H}(F(x \oplus \dot{K}) \oplus \beta) + \omega$, where β denotes the initial state of the register before updating with $F(x \oplus \dot{K})$, and ω denotes a zero-mean Gaussian random noise. Since $E(T_{\dot{K}}(x)) = \mathsf{H}(F(x \oplus \dot{K}) \oplus \beta)$, we omit the noise in the following, and $T_{\dot{K}}(x)$ turns into $\mathsf{H}(F(x \oplus \dot{K}) \oplus \beta)$. Naturally, for selection function D, we should have $D(X(i), K, j) = F_j(X(i) \oplus \dot{K}) \oplus \beta_j$. However, the item β_j, which is associated with the j^{th} bit of the initial state, is overlooked in the work of TO [37]. This flaw directly leads to the wrong formulation of single-bit DPA. And since the multi-bit DPA considered in TO is based on the combination and transformation of single-bit DPA, the validity of TO is also affected by this flaw. In [37], for an (n, m)-function F, the single-bit DPA is represented as $\Delta_{K,\dot{K}}(j) = \frac{1}{2^n} \sum_{i=1}^{m} Cor\left(F_j(x \oplus K), (F(x \oplus \dot{K}) \oplus \beta)_i\right)$. In the following, we will show the flaw in this formulation and fix it. Consistent with the assumption in [37], we assume that the initial state β is constant. It is realistic in some implementations with pre-charged logic, where the bus is cleared between each significant transferred value or when the previous operation concerning the bus is an opcode loading.

Proposition 2. *Let $F(x \oplus K)$ be a family of (n, m)-functions. Let β denote a constant initial state of a cryptographic system implementing functions $F(x \oplus K)$. If all functions $F(x \oplus K)$ are balanced, then for every pair $(K, \dot{K})$ and for every positive integer $j \leqslant m$, we have:*

$$\Delta_{K,\dot{K}}(j, \beta) = \frac{1}{2^n} \sum_{i=1}^{m} Cor\left((F(x \oplus K) \oplus \beta)_j, (F(x \oplus \dot{K}) \oplus \beta)_i\right) . \tag{5}$$

Proof. Due to Eq. (1), the power consumption $T_{\dot{K}}(x) = \mathsf{H}(F(x \oplus \dot{K}) \oplus \beta)$ can be rewritten as:

$$T_{\dot{K}}(x) = \frac{m}{2} - \frac{1}{2} \sum_{i=1}^{m} (-1)^{(F(x \oplus \dot{K}) \oplus \beta)_i} . \tag{6}$$

And we have $D(x, K, j) = F_j(x \oplus K) \oplus \beta_j$, which implies equalities $\sum_{i=1}^{2^n} D(x, K, j) = \#\, Supp\,(F_j(x \oplus K) \oplus \beta_j)$ and $\Sigma_{i=1}^{2n}(1 - D(x, K, j)) = 2^n - \#\, Supp\,(F_j(x \oplus K) \oplus \beta_j)$. Because we assume that each $F(x \oplus K)$ is balanced, it follows that cardinality of $Supp\,(F_j(x \oplus K) \oplus \beta_j)$ equals to 2^{n-1} for every pair (j, K). Thus, Eq. (2) applied for $N = 2^n$ implies the equation $\Delta_{K,\dot{K}}(j, \beta) = \frac{-1}{2^{n-1}}(\sum_{x \in \mathbb{F}_2^n}(1 - 2(F_j(x \oplus K) \oplus \beta_j))T_{\dot{K}}(x))$. Using Eq. (1), we obtain $\Delta_{K,\dot{K}}(j, \beta) = \frac{-1}{2^{n-1}}(\sum_{x \in \mathbb{F}_2^n}((-1)^{F_j(x \oplus K) \oplus \beta_j} T_{\dot{K}}(x)))$. This equation and Eq. (6) imply

$$\begin{aligned}\Delta_{K,\dot{K}}(j,\beta) =& \frac{-m}{2^n}\sum_{x\in\mathbb{F}_2^n}(-1)^{F_j(x\oplus K)\oplus\beta_j} \\ &+\frac{1}{2^n}\sum_{x\in\mathbb{F}_2^n}\sum_{i=1}^{m}(-1)^{(F_j(x\oplus K)\oplus\beta_j)\oplus\left(F_i(x\oplus\dot{K})\oplus\beta_i\right)}.\end{aligned} \tag{7}$$

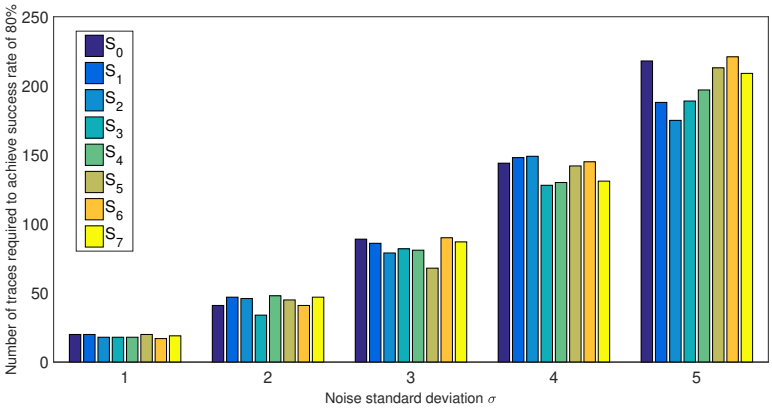
Due to the balancedness of $F(x\oplus K)$ and Proposition 2, the first summation in Eq. (7) is null for every guessed key K and for every bit j. Because the second summation in Eq. (7) equals to $\frac{1}{2^n}\sum_{i=1}^{m} Cor((F(x\oplus K)\oplus\beta)_j,(F(x\oplus\dot{K})\oplus\beta)_i)$, Eq. (7) and Eq. (5) are equivalent. □

3.2 One weakness of MTO

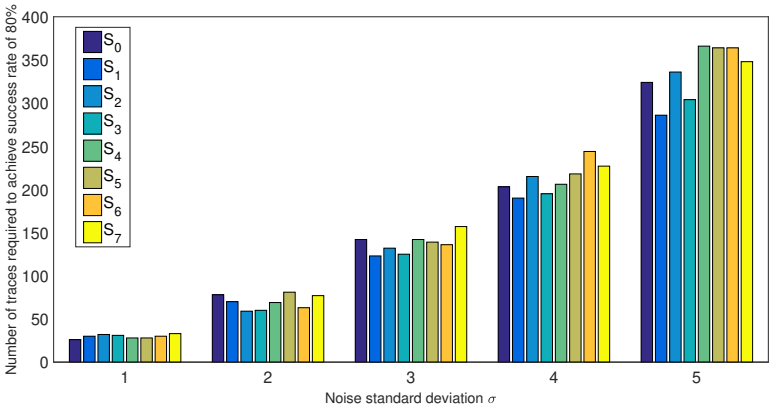
As described in Section 2.3.2, Chakraborty et al. [8] pointed out that TO ignores the correlation spectrum between paired coordinate functions of an S-box. At first, attempts were made in [8] to achieve a more precise measurement on the resistance of S-boxes by introducing items related to cross-correlation (i.e. $(-1)^{\beta_i}C_{F_i,F_j}(K\oplus\dot{K})$ for every $i\in\{1,\ldots,m\}$ and $i\neq j$) into TO. However, since the definitional flaw in TO is overlooked, there are still certain flaws in the items which were added to TO. Specifically, the correct form of cross-correlation items should be $(-1)^{\beta_i\oplus\beta_j}C_{F_i,F_j}(K\oplus\dot{K})$, which will be shown in Eq. (10), Section 4.1. For this reason, there are still certain limitations in the TO with added items (such as when β takes certain values, the value of TO is negative, which makes the definition unacceptable from the cryptanalyst's point of view). The work of MTO also discovered this limitation, but it mistakenly explained that the limitation is due to the insufficient power of the attacker. Hence it changed the ability of attackers and proposed MTO which considers the resistance of S-boxes towards the variant multi-bit DPA rather than original multi-bit DPA attack. The notion of MTO is correct from the perspective of formula, because when considering the variant multi-bit DPA, the flawed DPA formulation does not affect the validity of it. However, MTO did not virtually find the root cause of the flaw in TO, so it did not essentially fix it. Furthermore, both TO and MTO are defined under the Hamming weight leakage model, and yet Doget et al. have demonstrated that multi-bit DPA is actually more effective than the variant multi-bit DPA in Hamming weight leakage model [12]. Therefore, it seems not so reasonable to consider a variant multi-bit DPA in the notion of MTO.

In order to verify that multi-bit DPA is a more effective attack method than variant multi-bit DPA under Hamming weight leakage model, we perform simulated experiments using these two attack methods on eight S-box instances respectively. The chosen S-boxes are listed in the first 8 rows of Table 7 (Appendix A), which are representatives of the eight optimal classes of S-boxes fulfilling PRINCE S-box selection criteria up to affine equivalence [4]. We simulate the leakages as $\mathcal{L}(x\oplus\dot{K}) = \mathsf{H}(F(x\oplus\dot{K}))+\omega$, where $F(x\oplus\dot{K})$ denotes the S-box output, and ω denotes a Gaussian random variable with zero mean and standard deviation σ. In the experimental setup, the value of σ varies from

1 to 5. For each attack, we evaluate the minimum number of traces N required to achieve attack success rate of 80% as it has been shown to be a sound way to evaluate the efficiency of a side-channel attack [23, 38]. The attack results of multi-bit DPA and variant multi-bit DPA are shown in Fig. 1(a) and Fig. 1(b), respectively. It can be clearly seen that under the same conditions, the number of traces N required for multi-bit DPA is smaller than that for variant multi-bit DPA, and the gap between two attack methods becomes more obvious with the increase of noise level.



(a) Multi-bit DPA.



(b) Variant multi-bit DPA.

Fig. 1. Comparison of two kinds of DPA. The multi-bit DPA is involved in TO and RTO, and the variant multi-bit DPA is involved in MTO.

Further, we use an extreme example to illustrate the limitation of MTO. Consider a linear S-box with MTO value of 0 (although it cannot be used in practical for cryptographic reasons). According to the basic idea of MTO, it means that the linear S-box is completely resistant to the variant multi-bit DPA attack. However, using the multi-bit DPA distinguisher, one can easily obtain a

key candidate subset containing $\dot{K}$ and $\overline{\dot{K}}$ only, where $\dot{K}$ denotes the correct key and $\overline{\dot{K}}$ denotes the bit-reversed of $\dot{K}$. Thus, the linear S-box is prone to DPA attacks, although its MTO value is 0.

Through the above reasons, we demonstrated that MTO does overestimate the resistance of S-boxes being subjected to DPA attacks in Hamming weight leakage model. It is worth noting that it does not mean MTO is useless. Under other leakage models such as random linear model, MTO may still be an effective indicator. However, under the assumed Hamming weight leakage model, it is necessary to consider a more effective attack method, namely multi-bit DPA, to measure the DPA resistance of S-boxes in the worst case.

4 Redefining transparency order

Since the definitional flaw in TO and the weakness of MTO are presented in Section 3.1 and Section 3.2 respectively, in order to provide a sound quantitative security criterion, we amend TO and MTO, and propose the notion of revised transparency order (RTO) in this section.

4.1 The notion of revised TO

As discussed in Section 3.1, the root cause of the flaw in TO is that its single-bit DPA formulation is incorrect. Therefore, we fix this flaw and propose the notion of RTO based on the correct DPA formulation in this subsection.

According to Eq. (5), for a balanced $n \times m$ S-box F, the single-bit DPA can be rewritten as:

$$\Delta_{K,\dot{K}}(j,\beta) = \frac{1}{2^n}\sum_{i=1}^{m}(-1)^{\beta_i \oplus \beta_j}\mathcal{C}_{F_i,F_j}(K \oplus \dot{K})\,.$$

Combined with the description in Section 2.3, the multi-bit DPA $\delta_{K,\dot{K}}(\beta) = |\sum_{j=1}^{m}\Delta_{K,\dot{K}}(j,\beta)|$ can be calculated by:

$$\delta_{K,\dot{K}}(\beta) = \frac{1}{2^n}\left|\sum_{j=1}^{m}\sum_{i=1}^{m}(-1)^{\beta_i \oplus \beta_j}\mathcal{C}_{F_i,F_j}(K \oplus \dot{K})\right|\,. \tag{8}$$

Since $n \times m$ S-boxes we considered are balanced, we have $F_i \oplus F_j$ is balanced for every $i, j \in \{1, \ldots, m\}$ with $i \neq j$. Thus, we have $\mathcal{C}_{F_i,F_j}(0) = 0$ for every pair of distinct indices i and j. For $K = \dot{K}$ we have:

$$\delta_{\dot{K},\dot{K}}(\beta) = \frac{1}{2^n}\left|\sum_{j=1}^{m}(-1)^{\beta_j \oplus \beta_j}\mathcal{C}_{F_j,F_j}(0)\right| = \mathrm{m}\,. \tag{9}$$

From Eq. (8) and Eq. (9), and according to the basic idea of transparency order which measures the difference between the score for the correct key and the average score for the other hypotheses, we have:

$$\begin{aligned}\mathrm{RTO}(F,\beta) &= \frac{1}{2^n-1}\sum_{K\in\mathbb{F}_2^n-\{\dot{K}\}}\Big(\delta_{\dot{K},\dot{K}}(\beta)-\delta_{K,\dot{K}}(\beta)\Big)\\ &= \frac{1}{2^n-1}\sum_{a\in\mathbb{F}_2^{n^*}}\left(\delta_{0,0}(\beta)-\delta_{a,0}(\beta)\right)\\ &= m-\frac{1}{2^n\left(2^n-1\right)}\sum_{a\in\mathbb{F}_2^{n^*}}\left|\sum_{j=1}^{m}\sum_{i=1}^{m}(-1)^{\beta_i\oplus\beta_j}\mathcal{C}_{F_i,F_j}(a)\right|,\end{aligned} \tag{10}$$

where a plays the role of $K\oplus\dot{K}$ in Eq. (8).

Remark 1. We have $\mathrm{RTO}(F,\beta)=\mathrm{RTO}(F,\overline{\beta})$, where $\overline{\beta}$ denotes the bit-reversed of β.

By traversing the register initial state β, we eventually deduce the following new definition of RTO:

Definition 1. (Revised Transparency Order) Let F be a balanced $n\times m$ function. Its revised transparency order is the coefficient $\mathrm{RTO}(F)$ defined by:

$$\mathrm{RTO}(F)=\max_{\beta\in\mathbb{F}_2^m}\left(m-\frac{1}{2^{2n}-2^n}\sum_{a\in\mathbb{F}_2^{n^*}}\left|\sum_{j=1}^{m}\sum_{i=1}^{m}(-1)^{\beta_i\oplus\beta_j}\mathcal{C}_{F_i,F_j}(a)\right|\right). \tag{11}$$

Remark 2. The value of $\mathrm{RTO}(F)$ means the DPA resistance of the S-box in the worst case in the pre-charged logic (i.e., the value of β maximizes the RTO value). Thus, from designers' point of view, the value of β should be chosen carefully to minimize $\mathrm{RTO}(F,\beta)$, in which case the attacker's advantage is minimal. Similar to the work in [37], the value $\min_{\beta\in\mathbb{F}_2^m}\mathrm{RTO}(F,\beta)$ is denoted by $\mathrm{RTO}_{min}(F)$ and called *minimum revised transparency order*.

We exhibit a lower bound on $\mathrm{RTO}(F)$ in Appendix E. In this bound, all the cross correlation terms are replaced by Walsh spectrum values. This may make sense because the main cryptographic properties of S-boxes (nonlinearity, resiliency, balancedness and propagation criteria) are characterized through the Walsh transform.

In Table 1, a comparison of TO, MTO and RTO is listed. We analyze the soundness of the three notions from the perspective of leakage model, DPA formulation, S-box assumptions and power of adversaries. All the three notions are based on the Hamming weight leakage model, and both TO and RTO measure the resistance of S-boxes against a powerful DPA attack (i.e., multi-bit DPA). However, due to the flaw in DPA formulation and the impractical S-box assumption (i.e., the coordinates of S-boxes are uncorrelated with each other), the notion of TO has certain limitations. MTO fixed the flaw in S-box assumption, but the definitional flaw in DPA formulation is still overlooked. The validity

of MTO is not affected by this flaw because the variant multi-bit DPA attack is considered. However, since the variant multi-bit DPA attack is less powerful than multi-bit DPA, it underestimates the risk of S-boxes being subjected to DPA attacks and may result in inaccurate evaluation of S-boxes. Finally, we fix this definitional flaw in DPA formulation and propose the notion of RTO.

Table 1. Comparison of the theoretical basis of TO, MTO and RTO

	Leakage Model	**Formulation**	**S-box Assumptions**	**Power of Adversary**	**Soundness**
TO	HW	Flawed	Flawed	Powerful DPA	Flawed
MTO	HW	Flawed	Sound	Less powerful DPA	Flawed
RTO	HW	Correct	Sound	Powerful DPA	Sound

4.2 Affine invariance of RTO

It is well known that when an invertible affine transformation is applied before and after the S-box, the resistance of S-boxes against most classical cryptanalytic attacks remains unchanged. Based on this, studying the effect of affine transformations on other properties of S-boxes can simplify the evaluation of the security of S-boxes, and can also simplify the task of generating optimal S-boxes. Therefore, it is significant to exploring how the values of RTO change under affine transformations. Here we first give the definition of affine equivalence. Then the affine invariance of RTO is stated in Proposition 3.

For two $n \times n$ S-boxes F and G to be affine equivalent, the following equation needs to hold:

$$G(x) = B(F(A(x) \oplus d)) \oplus e\,, \tag{12}$$

where A and B are invertible $n \times n$ matrices and d, e are constants in $\mathbb{F}_2^n$.

Proposition 3. *Let $S(x)$ be an $n \times n$ S-box and $\mathrm{RTO}(S)$ be its revised transparency order. Then, the revised transparency order $\mathrm{RTO}(T)$ of $T(x) = S(A(x) \oplus d) \oplus e$ is equal to $\mathrm{RTO}(S)$, where A is an invertible $n \times n$ matrix and $d, e \in \{0,1\}^n$.*

Proof. Let $T(x) = B(S(A(x) \oplus d)) \oplus e$, i.e., $T(x)$ is any S-box that is affine equivalent to $S(x)$, where B is a nonsingular binary matrix. For simplicity, let

$$\mathrm{RTO}(T) = \max_{\beta \in \mathbb{F}_2^n} \left(n - \frac{Q_T}{2^{2n} - 2^n} \right),$$

where $Q_T = \sum_{a \in \mathbb{F}_2^{n*}} \left| \sum_{j=1}^{n} \sum_{i=1}^{n} (-1)^{\beta_i \oplus \beta_j} C_{T_i T_j}(a) \right|$. Then, it follows that,

$$
\begin{aligned}
Q_T &= \sum_{a\in\mathbb{F}_2^{n^*}} \left| \sum_{j=1}^{n}\sum_{i=1}^{n} (-1)^{\beta_i\oplus\beta_j} \sum_{x\in\mathbb{F}_2^n} (-1)^{(B(S(A(x)\oplus d))\oplus e)_i \oplus (B(S(A(x\oplus a)\oplus d))\oplus e)_j} \right| \\
&= \sum_{a\in\mathbb{F}_2^{n^*}} \left| \sum_{j=1}^{n}\sum_{i=1}^{n} (-1)^{\beta_i\oplus\beta_j\oplus e_i\oplus e_j} \sum_{y\in\mathbb{F}_2^n} (-1)^{(B(S_i(y)\oplus S_j(y\oplus A(a)))} \right| \\
&= \sum_{a\in\mathbb{F}_2^{n^*}} \left| \sum_{j=1}^{n}\sum_{i=1}^{n} (-1)^{\beta_i\oplus\beta_j\oplus e_i\oplus e_j} \sum_{y\in\mathbb{F}_2^n} (-1)^{(B(S_i(y)\oplus S_j(y\oplus u))} \right| \\
&= \sum_{a\in\mathbb{F}_2^{n^*}} \left| \sum_{j=1}^{n}\sum_{i=1}^{n} (-1)^{\beta'_i\oplus\beta'_j} \mathcal{C}_{BS_i,BS_j}(a) \right| ,
\end{aligned}
$$

which gives $\mathrm{RTO}(T) = \mathrm{RTO}(S)$ if B is the identity matrix, where $\beta' \in \mathbb{F}_2^n$ satisfies Eq. (11). □

5 Practical soundness of RTO: case studies

To evaluate the validity and soundness of RTO, we perform simulated and practical attacks against 4×4 and 8×8 S-boxes, respectively.

5.1 Validity of RTO: real world 4×4 S-boxes

In this subsection, we compare the notions of TO, MTO and RTO to illustrate the validity of RTO. The experiments correspond to multi-bit DPA attacks against nine 4×4 S-boxes, which are actually used in cryptographic algorithms. The nine S-boxes are listed in Table 2 [41, 22, 3, 42, 4].

We use difference value indicator (DVI) to evaluate the validity of the three transparency order. The value of DVI can be calculated according to

$$
\mathrm{DVI}(F,\ \mathrm{trace}\ ) = \frac{1}{2^n-1} \sum_{K\in\mathbb{F}_2^n-\{\dot{K}\}} \left(\delta_{\dot{K},\dot{K}} - \delta_{K,\dot{K}}\right) ,
$$

where $\delta_{\dot{K},\dot{K}}$ denotes the score of the correct key, and $\delta_{K,\dot{K}}$ denotes the score of key hypothesis K. In essence, the DVI and (revised) transparency order are based on the same basic idea, except that DVI is calculated using collected traces.

Simulated experiments. In simulated experiments, leakages are simulated as

$$
\mathcal{L}(x \oplus \dot{K}) = \mathsf{H}(F(x \oplus \dot{K}) \oplus \beta) + \omega \,,
$$

where $F(x \oplus \dot{K})$ denotes the sensitive variable, and ω denotes a Gaussian random variable centered in zero with a standard deviation σ. The value β

Table 2. Nine 4×4 S-boxes which are actually used in cryptographic algorithms

Algorithm	Notation	S-box
ICEBERG	$\text{ICEBERG}_{\text{S0}}$	13, 7, 3, 2, 9, 10, 12, 1, 15, 4, 5, 14, 6, 0, 11, 8
	$\text{ICEBERG}_{\text{S1}}$	4, 10, 15, 12, 0, 13, 9, 11, 14, 6, 1, 7, 3, 5, 8, 2
mCrypton	$\text{mCrypton}_{\text{S0}}$	4, 15, 3, 8, 13, 10, 12, 0, 11, 5, 7, 14, 2, 6, 1, 9
	$\text{mCrypton}_{\text{S1}}$	1, 12, 7, 10, 6, 13, 5, 3, 15, 11, 2, 0, 8, 4, 9, 14
	$\text{mCrypton}_{\text{S2}}$	7, 14, 12, 2, 0, 9, 13, 10, 3, 15, 5, 8, 6, 4, 11, 1
	$\text{mCrypton}_{\text{S3}}$	11, 0, 10, 7, 13, 6, 4, 2, 12, 14, 3, 9, 1, 5, 15, 8
PRESENT	PRESENT	12, 5, 6, 11, 9, 0, 10, 13, 3, 14, 15, 8, 4, 7, 1, 2
PRINCE	PRINCE	11, 15, 3, 2, 10, 12, 9, 1, 6, 7, 8, 0, 14, 5, 13, 4
RECTANGLE	RECTANGLE	6, 5, 12, 10, 1, 14, 7, 9, 11, 0, 3, 13, 8, 15, 4, 2

corresponds to the initial state of the register before updating with $F(x \oplus \dot{K})$. According to the discussion in previous sections, we assume that β is a constant and can be set by the designer. For clear comparison, the value of β for each S-box implementation is set to zero. The corresponding values of $\text{TO}(F, \beta)$, $\text{MTO}(F, \beta)$ and $\text{RTO}(F, \beta)$ (denoted as $\text{TO}_0(F)$, $\text{MTO}_0(F)$, $\text{RTO}_0(F)$, respectively) are calculated.

Attacks are performed on 500,000 simulated traces with different leakage noise levels ($\sigma = 1$, $\sigma = 2$, and $\sigma = 5$). The DVI values of each S-box in the three simulation attacks with different noise levels are denoted as DVI_{SA1}, DVI_{SA2} and DVI_{SA3}, respectively. The values of DVI and three transparency order for the nine S-boxes are shown in Fig. 2.

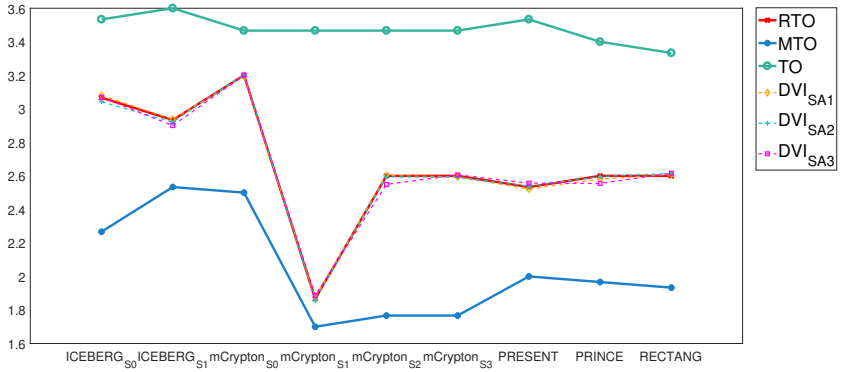


Fig. 2. Values of DVI, TO, MTO and RTO of nine S-boxes.

Simulated results. It can be clearly seen that the values of DVI for the nine S-boxes are substantially consistent with RTO, which verifies the validity

of RTO. In contrast, the obvious difference between the values of TO and DVI shows the limitation of TO, because both TO and RTO quantify the resistance of S-boxes against multi-bit DPA attack under Hamming weight leakage model. Furthermore, it can be observed that the values of MTO for all the nine S-boxes are lower than DVI, which confirms MTO does underestimate the risk of S-boxes being subjected to DPA attacks. And the inconsistency between the values of MTO and DVI (such as $\text{ICEBERG}_{\text{S0}}$ and $\text{ICEBERG}_{\text{S1}}$) also indicates that, in some cases, evaluating the DPA resistance of S-boxes in terms of MTO may result in inaccurate results.

Practical experiments. In practical experiments, all the nine S-boxes are implemented on a FunCard with an Atmel ATmega 163 microprocessor. Same as the simulated experiments, we set the register initial state β equals to 0. The traces are obtained from a SASEBO-W platform with a lower pass filter (BLP-90+) and an amplifier, and the sampling rate is set to 20MHz. 4,000 points around the sensitive operations are taken to attack. Similar to the simulated experiments above, we calculate the value of DVI for each S-box based on 3,000 collected traces. In order to study the performance of three transparency order with different noise levels, the attacks are performed based on the raw traces and traces with added Gaussian noise ($\sigma = 2$ and $\sigma = 3$), respectively. The DVI values of each S-box in the three attacks with different noise levels are denoted as DVI_{PA1}, DVI_{PA2} and DVI_{PA3}. Since the value of DVI is directly related to the magnitude of collected traces, we calculate the Pearson correlation coefficients between the values of three transparency order and DVI based on the nine S-boxes. The results are listed in Table 3.

Table 3. The Pearson correlation coefficients between the values of three transparency order and DVI

Notion \ DVI	$\textbf{DVI}_{\text{PA1}}$	$\textbf{DVI}_{\text{PA2}}$	$\textbf{DVI}_{\text{PA3}}$
TO	0.15	0.01	0.06
MTO	0.81	0.67	0.72
RTO	**0.85**	**0.89**	**0.80**

Practical results. It can be observed that the Pearson correlation coefficients between the values of RTO and DVI are the highest in all the three attack groups, which shows the superiority of RTO. However, the values of RTO and DVI are not exactly matched as in the simulated experiments. We argue that the main reason is the number of the traces used for attacks is limited, because in the notion of RTO, it is assumed that the number of traces is sufficient so that the noise can be omitted. Besides, the leakages in real environment do not fully satisfy Hamming weight leakage model and the noise does not fulfill Gaussian noise assumption, which may also lead to inconsistent results.

Remark 3. We also compare the notions of TO, MTO and RTO based on the 8×8 S-boxes. Since the results are consistent with that of the 4×4 S-boxes, they are not specifically shown here.

5.2 Soundness of RTO

5.2.1 Real world 4×4 S-boxes

In Section 5.1, through simulated and practical experiments, the validity of RTO has been confirmed by comparing the values of RTO and DVI indicators of nine 4×4 S-boxes. Although DVI could be used to quantify the DPA resistance of S-boxes, it is not a metric commonly used in the field of side-channel analysis such as success rate and guess entropy. Therefore, in this section, we demonstrate the soundness of RTO by evaluating the minimum number of traces required for achieving attack success rate of 80%. The experimental setup of simulated and practical attacks is the same as in Section 5.1, and results are reported in Fig. 3 and Fig. 4, respectively.

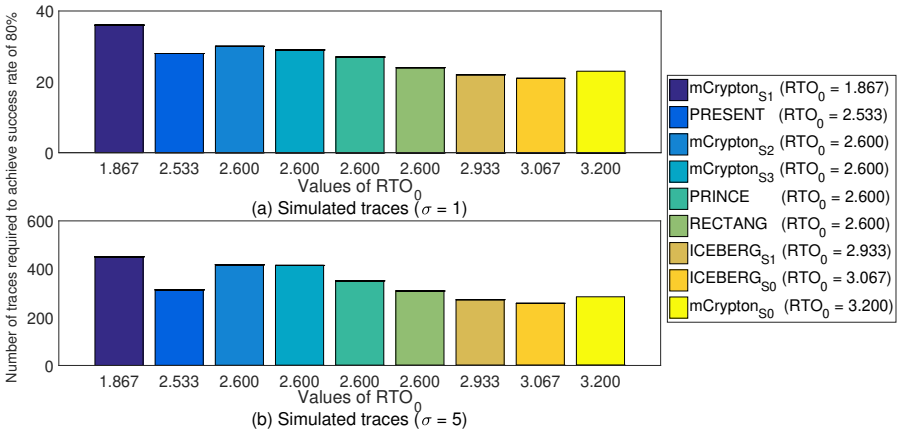


Fig. 3. Simulated multi-bit DPA attacks on nine 4×4 S-boxes.

Simulated results. From Fig. 3, it is clear that the results of simulated experiments are basically consistent with theoretical analysis. In other words, S-boxes with lower RTO_0 values are more resistant against DPA. Specifically, when the difference of the RTO_0 values of the two S-boxes is relatively large, the S-box with a lower RTO_0 value is generally more resistant to DPA attack. The S-box (e.g. $\mathrm{mCrypton}_{S1}$) with the lowest RTO_0 value requires the largest number of traces for successful attacks. In conclusion, the results confirm that RTO does reflects the DPA resistance of an S-box implementation. However, one may also note that the RTO alone does not fully capture the resistance of S-boxes against DPA, because the number of traces required for success attack of S-boxes with the same RTO_0 value are different more or less (such as

mCrypton$_{S2}$, mCrypton$_{S3}$, the S-box of PRINCE and the S-box of RECTANG). We argue that the main reason for this phenomenon is the different perspectives of RTO and success rate metric when quantifying the DPA resistance of S-boxes. As introduced in Section 2.3.1, the basic idea of RTO is quantifying the difference between the score for the correct key and the average score for the other hypotheses, however, the success rate metric quantifies the number of successful attacks (i.e., the number of attacks in which the correct key is ranked first) in all attacks performed.

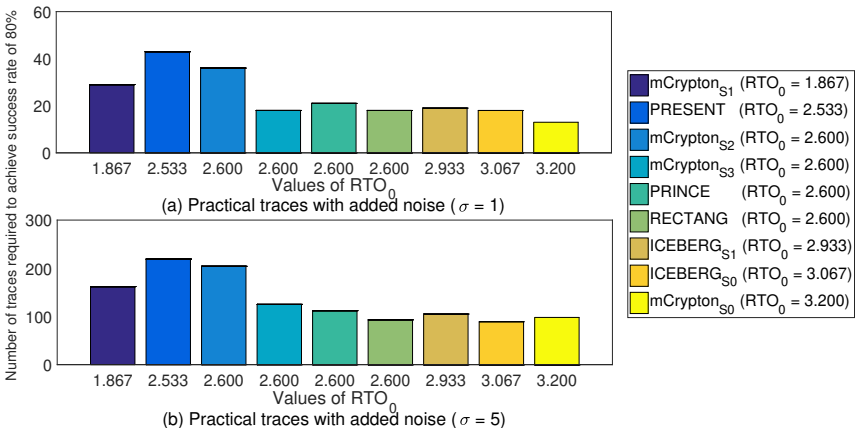


Fig. 4. Practical multi-bit DPA attacks on nine 4×4 S-boxes.

Practical results. In Fig. 4, for most S-box examples, those S-boxes with lower RTO_0 values still have higher DPA resistance in real environments. However, one may also note that for certain S-boxes such as PRESENT and mCrypton $_{S2}$, the results obtained are not consistent with simulated results. Besides the different perspectives of RTO and success rate, we infer the reasons for the inconsistent results are the same as discussed in Section 5.1. So far, we can conclude that the soundness RTO is still true in practical attacks.

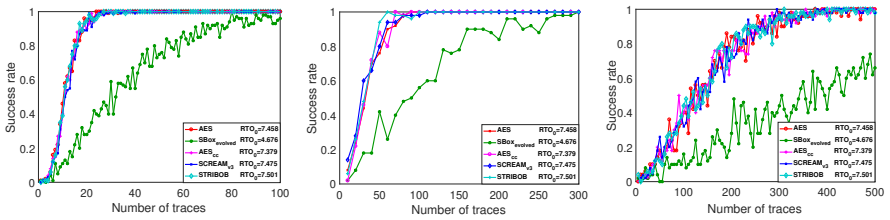
5.2.2 8×8 S-boxes

We perform DPA attacks against 8×8 S-boxes to verify the soundness of RTO when the size of S-boxes is changed. The five S-boxes are as follows, three of which are used in cryptographic algorithms and the other two are constructed S-boxes.

- S-box of AES [39];
- $\text{SBox}_{\text{evolved}}$ [35], which reaches the best confusion coefficient variance, but has nonlinearity 98 and δ-uniformity 12 (AES has nonlinearity 112 and δ-uniformity 4);

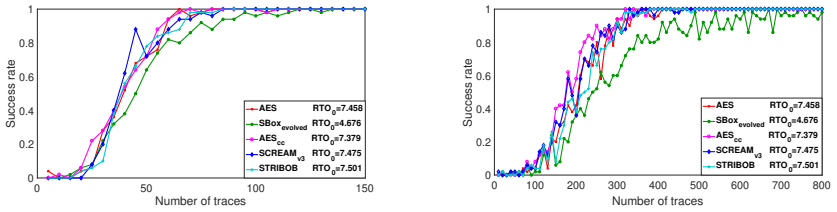
- AES_{cc} [35], which is the affine transformation of AES S-box with improved confusion coefficient;
- S-box of $\text{SCREAM}_{\text{v3}}$ [16];
- S-box of STRIBOB [40].

Simulated and practical experiments. Similar to Section 5.1, the initial state β of each S-box implementation is set to zero, and the corresponding $\text{RTO}(\text{F}, \beta)$ value (denoted as $\text{RTO}_0(\text{F})$) is calculated. In simulated experiments, standard deviation σ of noise equals to 0, 2 and 5, respectively. And in practical experiments, the experimental setup is the same as in Section 5.1. The attacks are performed on the raw traces and traces with Gaussian noise added ($\sigma = 2$), respectively. For each attack, we use success rate as a metric. The results are shown in Fig. 5 and Fig. 6.



(a) Simulated traces ($\sigma = 0$) (b) Simulated traces ($\sigma = 2$) (c) Simulated traces ($\sigma = 5$)

Fig. 5. Simulated DPA attacks on five 8×8 S-boxes.



(a) Practical traces (b) Practical traces with added noise ($\sigma = 2$)

Fig. 6. Practical DPA attacks on five 8×8 S-boxes.

Simulated and practical results. It can be clearly seen that attack results are consistent with theoretical analysis in both simulated and practical experiments. Except for the $\text{SBox}_{\text{evolved}}$, the RTO_0 values of the other four S-boxes are very close to each other. Correspondingly, the implementation of $\text{SBox}_{\text{evolved}}$ is more difficult to attack successfully. Based on the above results, we draw the conclusion that it is sound to quantify the DPA resistance of S-boxes with different sizes in terms of RTO.

6 Recommendations on selecting optimal 4×4 S-boxes

As an indicator to measure the DPA resistance of S-boxes, a specific application of RTO is to guide the construction of optimal S-boxes. To generate S-boxes with high DPA resistance, one feasible method is selecting S-boxes with low RTO values from those S-boxes that fulfill cryptographic criteria such as high nonlinearity and high algebraic degree. Under affine transformations, the properties of most cryptographic criteria have been studied relatively thoroughly, and with respect to linear and differential cryptanalyses, optimal 4×4 S-boxes up to affine equivalence are shown in [21]. Therefore, this section takes 4×4 S-boxes as an example to illustrate how to select optimal S-boxes in terms of RTO. We first present the distribution of RTO values for sixteen optimal affine equivalence classes, and then illustrate the important influence of register initial state β. Finally, we explore the selection of optimal S-boxes and make some recommendations from the perspective of RTO.

6.1 RTO values of 4×4 S-boxes in optimal classes

In [21], Leander et al. classified all optimal 4×4 S-boxes into 16 classes up to affine equivalence with respect to linear and differential cryptanalyses. Representatives for all 16 optimal classes proposed in [21] are listed in Table 7 of Appendix A. Note that we reorder the rank of these S-boxes according to the algebraic degree of them, where each of the 15 non-zero component functions of S_0 to S_7 has algebraic degree 3, while S_8 to S_{15} do not fulfill this criteria. This classification simplifies the task of generating optimal 4×4 S-boxes since it is well known that the resistance of S-boxes against most cryptanalyses remains unchanged under affine transformations. However, it has been shown in Section 4.2 that the RTO values of S-boxes are not always affine invariant under all types of affine transformations. Therefore, it is necessary to conduct an exhaustive search in the 16 optimal classes and explore the frequency distribution of RTO values.

According to Proposition 3, RTO remains affine invariant only under certain affine transformations which are based on $S_2(x) = S_1(A(x) \oplus d) \oplus e$. Therefore, we can apply transformations in the form of $S_2(x) = B(S_1(x))$ to conduct an exhaustive search for each optimal affine equivalence class, where B denotes an invertible $n \times n$ matrix. Note that this affine transformation is the special form of Eq. (12) where constants d and e equal to 0 and matrix A is the identity matrix. TO and MTO are demonstrated to have similar properties [13, 34].

Results of exhaustive search for all 16 optimal classes' lower and upper bounds are given in Table 4. Additionally, the frequency distribution of RTO values is shown in Fig. 7.

It can be observed that there are 11 different RTO values for all optimal S-boxes, and there are four classes that reach the minimal value of 2.6. Among all S-boxes in the optimal classes, only about 0.1% of them reach this value. However, none of these S-boxes have high algebraic degree, which is a frequently used criterion for good S-boxes. For S-boxes with high algebraic degree, the minimal RTO value that can be obtained is 2.933, and four classes reach this

Table 4. RTO values of optimal S-boxes

S-box	$\#deg(S_b) = 3$[1]	RTO value		S-box	$\#deg(S_b)=3$	RTO value	
		Min	Max			Min	Max
S_0	15	3.133	3.333	S_8	12	2.600	3.533
S_1	15	2.933	3.533	S_9	12	2.600	3.533
S_2	15	3.067	3.533	S_{10}	12	2.867	3.533
S_3	15	3.000	3.533	S_{11}	12	2.600	3.533
S_4	15	2.933	3.533	S_{12}	12	2.933	3.533
S_5	15	2.933	3.533	S_{13}	12	2.933	3.533
S_6	15	3.067	3.533	S_{14}	12	2.933	3.533
S_7	15	2.933	3.533	S_{15}	12	2.600	3.533

[1] Number of $b \in \mathbb{F}_2^4 \backslash \{0\}$ such that $deg(S_b) = 3$.

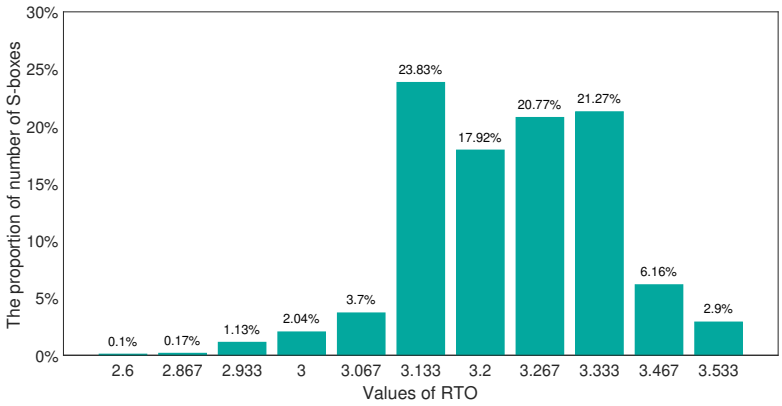


Fig. 7. Frequency distribution of RTO values of optimal S-boxes.

value. Except for class S_0, the maximal value of all the remaining 15 classes is 3.533. In order to facilitate the comparison, results of the exhaustive search according to TO and MTO are given in Appendix C.

As mentioned in *Remark 2*, $\mathrm{RTO}_{\min}$ value is equal to the minimum value of $\mathrm{RTO}(F, \beta)$ obtained by traversing the register initial state β. For pre-charged platforms, it is reasonable to assume that β is a constant and can be set by the designer. Therefore, it is meaningful to explore the frequency distribution of $\mathrm{RTO}_{\min}$ values. Similar to RTO, we apply transformations in the form of $S_2(x) = B(S_1(x))$ to conduct an exhaustive search for each optimal affine equivalence class, and results are given in Table 5 and Fig. 8, respectively.

It can be seen that there are 10 different RTO_{min} values for all optimal S-boxes, and unlike the distribution of RTO values, each class can reach the minimal value of 1.867. Among all S-boxes, about 28% of them reach this value. That is, if the value of register state β can be set by the designer, then more than a quarter of the S-boxes are optimal in terms of RTO_{min}. Similarly, results of the exhaustive search according to MTO_{min} are given in Appendix D. We

Table 5. RTO_{min} values of optimal S-boxes

S-box	$\#deg(S_b)$=3	RTO_{min} value		S-box	$\#deg(S_b)$=3	RTO_{min} value	
		Min	Max			Min	Max
S_0	15	1.867	2.933	S_8	12	1.867	3.133
S_1	15	1.867	2.933	S_9	12	1.867	3.133
S_2	15	1.867	2.933	S_{10}	12	1.867	3.067
S_3	15	1.867	2.933	S_{11}	12	1.867	3.067
S_4	15	1.867	2.933	S_{12}	12	1.867	2.933
S_5	15	1.867	2.933	S_{13}	12	1.867	2.933
S_6	15	1.867	2.867	S_{14}	12	1.867	2.933
S_7	15	1.867	2.933	S_{15}	12	1.867	3.067

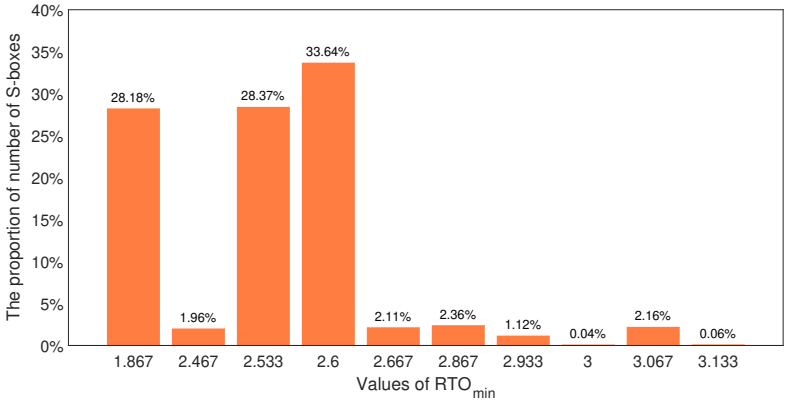


Fig. 8. Frequency distribution of RTO_{min} values of optimal S-boxes.

do not give the results for TO_{min}, because the TO_{min} values of all optimal S-boxes are negative, which confirms that the notion of TO does have unacceptable limitations.

6.2 Effect of β on RTO of S-boxes

As can be seen from the above analysis, the difference between the range of RTO and RTO_{min} values is obvious for all optimal S-boxes. Therefore, it can be inferred that the register state β significantly affects the DPA resistance of an S-box. This effect will be verified by simulated and practical experiments in the following.

We take S-boxes with high algebraic degree as examples, that is, the S-boxes are selected from S_0 to S_7 classes. Since there are 7 different RTO_{min} values for optimal S-boxes belonging to class S_0 to S_7, we first divide the S-boxes into 7 groups based on their RTO_{min} values. Then we randomly select an S-box as a representative in each group. The selected S-boxes are listed in Table 8 of Appendix B.

Simulated experiments. We perform multi-bit DPA simulated attacks against the seven selected S-boxes in two different experimental setups. The leakages are simulated as $\mathcal{L}(x \oplus \dot{K}) = \mathsf{H}(F(x \oplus \dot{K}) \oplus \beta) + \omega$. The value β corresponds to the initial state of the register before updating with $F(x \oplus \dot{K})$. In the two experimental setups, we set β to reach the value of RTO_{min} and RTO respectively, and the corresponding β values are denoted as β_{min} and β_{max}. The integer values of β_{min} and β_{max} of each S-box are shown in Table 6. Attacks are performed at a relatively high level of leakage noise (standard deviation $\sigma = 8$) to make the results more obvious. Similar to Section 3 and Section 5, we estimated the minimum number of traces N required to achieve an 80% attack success rate. Results are reported in Fig. 9.

Table 6. β_{min} and β_{max} values of 7 S-boxes

S-box	β_{min}	β_{max}
G_0	1	2
G_1	0	1
G_2	4	1
G_3	0	5
G_4	7	1
G_5	3	6
G_6	0	3

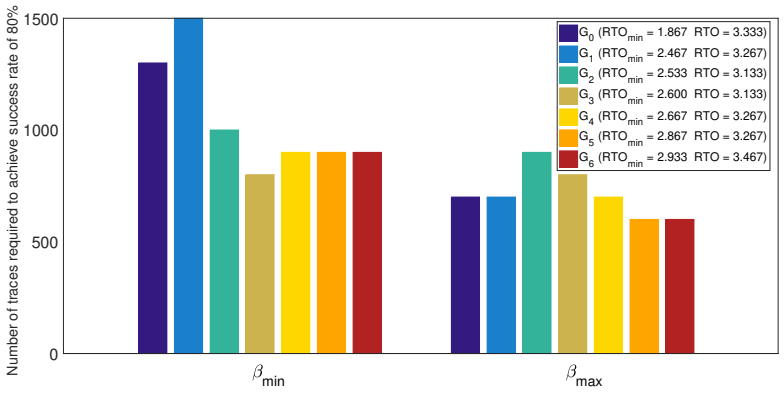
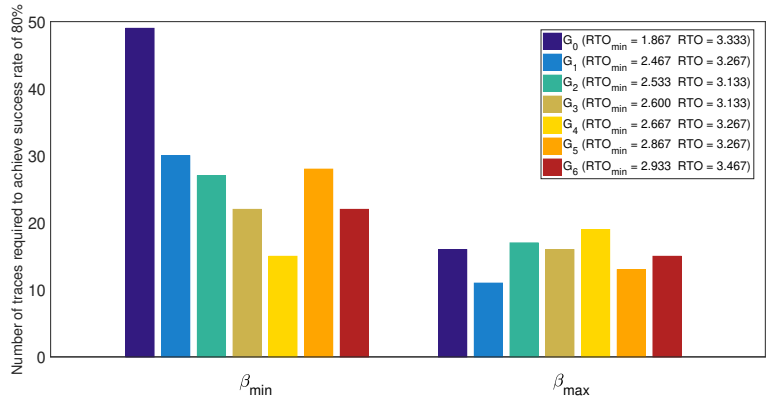


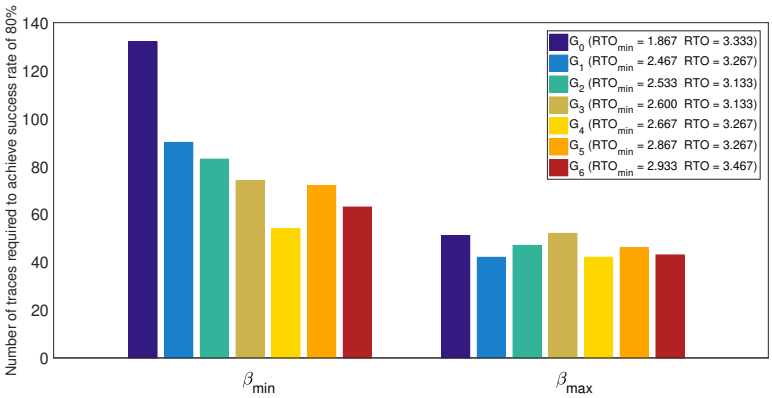
Fig. 9. Multi-bit DPA attacks on simulated traces for 7 S-boxes.

Practical experiments. In practical experiments, all experimental settings are the same as in Section 5. And we also set the register initial state β equals to β_{min} and β_{max}, respectively. The results are shown in Fig. 10(a). We also

launch DPA attacks on the traces with added Gaussian noise ($\sigma = 2$) for a more intuitive observation. The results are shown in Fig. 10(b).



(a) Practical traces.



(b) Practical traces with added noise ($\sigma = 2$).

Fig. 10. Multi-bit DPA attacks on practical traces for 7 S-boxes.

Simulated and practical results. The results of simulated and practical experiments are consistent in most cases, and small differences might be caused by the noise in practical experiments not fully satisfying the Gaussian noise. It can be observed that when the initial state β is set to β_{min}, the number of traces required for a successful attack is generally higher than that needed when β equals to β_{max}. Moreover, in both simulated and practical attacks, for the S-box G_0, the number of needed traces when $\beta = \beta_{min}$ gets approximately 2 times that of $\beta = \beta_{max}$. Therefore, the register state β does affect the DPA resistance of S-boxes. However, one may also notice that for some S-boxes such as G_4, there is no obvious difference in the number of traces required for a successful attack when β is equal to β_{min} and β_{max}, respectively. Even in extreme cases, the number of needed traces when $\beta = \beta_{min}$ gets lower than that of $\beta = \beta_{max}$.

We argue that the reason for this mismatch is the same as that analyzed in Section 5. To sum up, for platforms with reset state, designers should set the value of β carefully to minimize $\mathrm{RTO}(\mathrm{F}, \beta)$, thereby effectively improving the DPA resistance of S-box implementations.

6.3 Recommendations on selecting optimal 4×4 S-boxes

Based on previous analysis, we will give some recommended guidelines on how to select optimal S-boxes from the perspective of RTO. In this subsection, we mainly discuss the following three situations:

(1) For platforms with pre-charged logic, where β is a constant and can be set by the designer, the S-boxes with the minimal $\mathrm{RTO}_{\min}$ value should be selected among the S-boxes that fulfill the cryptographic algorithm criteria. And the value of β should be set carefully to reach $\mathrm{RTO}_{\min}$. Taking the PRINCE algorithm as an example, it requires S-boxes to have high algebraic degree. Hence, designers should select the S-boxes with an $\mathrm{RTO}_{\min}$ value of 1.867 in the classes of S_0 to S_7 in Table 2.

(2) For cryptographic implementations with Hamming weight leakage model (i.e., the register state β is 0 before the substitution operation), the S-boxes with the minimum $\mathrm{RTO}_{\min}$ value and the corresponding β_{min} value of 0 should be selected. For PRINCE algorithm, designers should select the S-boxes with initial state $\beta_{min} = 0$ in those S-boxes with an $\mathrm{RTO}_{\min}$ value of 1.867.

(3) When the designer cannot reset the register state β of the cryptographic implementations and considers the DPA resistance of S-boxes in the worst case, the S-boxes with the minimum RTO value should be selected. For PRINCE algorithm, designers should select the S-boxes with an RTO value of 2.933 in the S_0 to S_7 classes.

We emphasize that the recommendations for selecting optimal S-boxes are only from the perspective of RTO. When selecting S-boxes which are used in cryptographic implementations, it is not enough to consider RTO alone, and other metrics such as success rate and guess entropy need to be considered comprehensively. In addition, for S-boxes with other sizes such as 8×8 S-boxes, there is no such classification based on affine equivalence. Therefore, how to select optimal S-boxes with other sizes is not discussed in this work. Like Picek et al. did in [32], some heuristic methods could be used to search for optimal S-boxes.

7 Conclusions and future work

In this paper, we revisit the notions of TO and MTO, and spot a definitional flaw in TO, which was not pointed out in MTO but seriously affected the soundness of TO. The work of MTO did not discover this flaw virtually but accidentally bypassed it by applying a less powerful DPA attack. We argue that MTO overestimates the resistance of S-boxes against DPA attacks because the variant multi-bit DPA attack considered in MTO is not that powerful as one may think.

Then, we fix these flaws and propose the notion RTO. The soundness of RTO is demonstrated through simulated and practical experiments. The results also confirm that RTO is a valuable criterion to evaluate DPA resistance of S-boxes. Furthermore, the distribution of RTO values in sixteen optimal affine equivalence classes of 4×4 S-boxes is explored. Finally, some recommendations on how to select optimal 4×4 S-boxes in practical implementations are proposed from the perspective of RTO. However, we must emphasize that RTO is one of the critical metric for S-box selection since it can only provide a perspective to measure the DPA resistance, so it is not enough to consider RTO along when designing a cryptographic algorithm.

Since RTO is expected to be a practical evaluation tool for evaluating the DPA resistance of S-boxes, it is significant to explore the fast computation of RTO in the future. In [14], Fan et al. presented a fast implementation method for TO. However, this method is not feasible for RTO at present, and is also not feasible for MTO, neither. Furthermore, with the development of the cryptanalysis techniques, there appears a trend of using larger size S-boxes in emerging block ciphers. Therefore, the limitation of computational complexity may restrict the practicability of RTO, and how to calculate RTO in a short time may become an important issue. In addition, we believe that it would be important to figure out how to extend RTO to more attacks (e.g. template attacks and regression attacks) under variant leakage models (e.g. Hamming distance model and linear leakage model), which is far apart from the DPA under HW model since the practical attacks and leakage models get more advanced. And the construction of optimal S-boxes of different sizes with small RTO is also an open problem.

Acknowledgment

This work is supported in part by National Natural Science Foundation of China (No.61632020, No.61772520) and Beijing Natural Science Foundation (No. 4192067).

A List of representatives for 16 optimal classes up to affine equivalence

In [21], Leander et al. classified all optimal 4×4 S-boxes into 16 classes up to affine equivalence with respect to linear and differential cryptanalyses. Representatives for all 16 optimal classes proposed in [21] are listed in Table 7. Note that we reorder the rank of these S-boxes according to the algebraic degree of them, where each of the 15 non-zero component functions of S_0 to S_7 has algebraic degree 3, while S_8 to S_{15} do not fulfill this criteria.

B List of the 4×4 S-boxes used in Section 6.2

The seven S-boxes used in Section 6.2 are listed in Table 8. These S-boxes are selected from S_0 to S_7 classes in Table 7, which have high algebraic degree. Since

Table 7. Representatives for all 16 classes of optimal 4×4 S-boxes

S_0	0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 5, 3, 10, 14, 11, 9
S_1	0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 9, 11, 10, 14, 5, 3
S_2	0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 11, 9, 10, 14, 3, 5
S_3	0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 11, 9, 10, 14, 5, 3
S_4	0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 14, 11, 10, 9, 3, 5
S_5	0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 11, 10, 5, 9, 12, 3
S_6	0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 11, 10, 9, 3, 12, 5
S_7	0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 12, 9, 5, 11, 10, 3
S_8	0, 1, 2, 13, 4, 7, 15, 6, 8, 11, 12, 9, 3, 14, 10, 5
S_9	0, 1, 2, 13, 4, 7, 15, 6, 8, 11, 14, 3, 5, 9, 10, 12
S_{10}	0, 1, 2, 13, 4, 7, 15, 6, 8, 11, 14, 3, 10, 12, 5, 9
S_{11}	0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 9, 5, 10, 11, 3, 12
S_{12}	0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 11, 3, 5, 9, 10, 12
S_{13}	0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 11, 5, 10, 9, 3, 12
S_{14}	0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 12, 11, 3, 9, 5, 10
S_{15}	0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 12, 11, 9, 3, 10, 5

there are 7 different RTO_{min} values for optimal S-boxes belonging to class S_0 to S_7, the S-boxes are divided into 7 groups in terms of their RTO_{min} values. Then an S-boxes is randomly selected as a representative from each group.

Table 8. 4×4 S-boxes used in Section 6.2

G_0	0, 2, 1, 13, 7, 4, 12, 6, 8, 14, 15, 10, 5, 11, 9, 3
G_1	0, 12, 14, 9, 8, 10, 7, 6, 13, 11, 5, 1, 4, 15, 3, 2
G_2	0, 9, 2, 10, 15, 4, 8, 13, 12, 1, 3, 5, 6, 7, 14, 11
G_3	0, 7, 6, 12, 9, 8, 10, 15, 2, 13, 11, 5, 14, 3, 4, 1
G_4	0, 10, 11, 14, 9, 8, 5, 2, 13, 15, 4, 7, 3, 12, 6, 1
G_5	0, 3, 9, 8, 6, 12, 1, 15, 13, 2, 11, 14, 5, 7, 4, 10
G_6	0, 1, 7, 12, 4, 2, 11, 3, 9, 10, 13, 8, 5, 15, 14, 6

C TO and MTO values of 4×4 S-boxes in optimal classes

The TO values for all 16 optimal classes' lower and upper bounds are given in Table 9, and the frequency distribution of all TO values for all 16 optimal classes is shown in Fig. 11. The corresponding results for the MTO are shown in Table 10 and Fig. 12, respectively.

It can be observed that there are 9 different TO values and 30 different MTO values for all optimal S-boxes, respectively. The minimum and maximum values of TO, MTO and RTO are different. For the property of TO , there are three classes (i.e., S_8, S_9 and S_{11}) that reach the minimal value of 3.2, while for MTO,

Table 9. TO values of optimal S-boxes

S-box	$\#deg(S_b)$=3	TO value		S-box	$\#deg(S_b)$=3	TO value	
		Min	Max			Min	Max
S_0	15	3.467	3.733	S_8	12	3.200	3.733
S_1	15	3.400	3.733	S_9	12	3.200	3.733
S_2	15	3.400	3.733	S_{10}	12	3.267	3.733
S_3	15	3.333	3.733	S_{11}	12	3.200	3.733
S_4	15	3.400	3.733	S_{12}	12	3.267	3.733
S_5	15	3.333	3.733	S_{13}	12	3.267	3.733
S_6	15	3.400	3.667	S_{14}	12	3.267	3.733
S_7	15	3.333	3.733	S_{15}	12	3.267	3.733

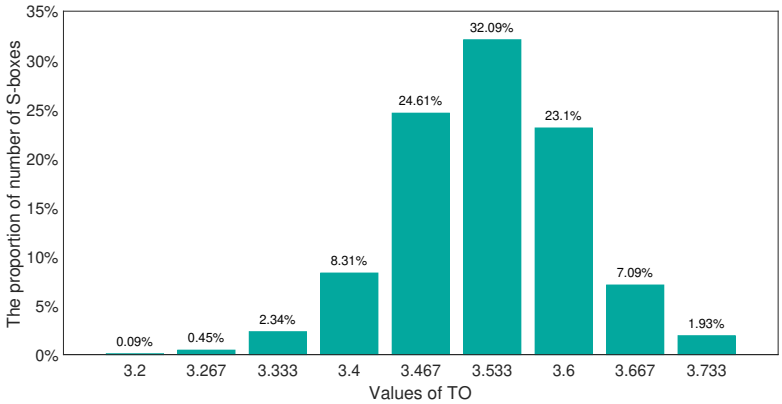


Fig. 11. Frequency distribution of TO values of optimal S-boxes.

Table 10. MTO values of optimal S-boxes

S-box	$\#deg(S_b)$=3	MTO value		S-box	$\#deg(S_b)$=3	MTO value	
		Min	Max			Min	Max
S_0	15	2.400	2.800	S_8	12	2.067	3.000
S_1	15	2.300	2.833	S_9	12	1.900	2.800
S_2	15	2.333	2.933	S_{10}	12	2.033	2.867
S_3	15	2.233	2.733	S_{11}	12	2.033	2.867
S_4	15	2.267	2.700	S_{12}	12	2.167	2.800
S_5	15	2.233	2.667	S_{13}	12	2.167	2.767
S_6	15	2.333	2.833	S_{14}	12	2.200	2.933
S_7	15	2.267	2.900	S_{15}	12	2.133	2.900

there is only one class (i.e., S_9) that reaches the minimal value of 1.9. For TO, except for class S_6, the maximal value of all the remaining 15 classes is 3.733. While for MTO, the maximal value of each class is different in most cases. In

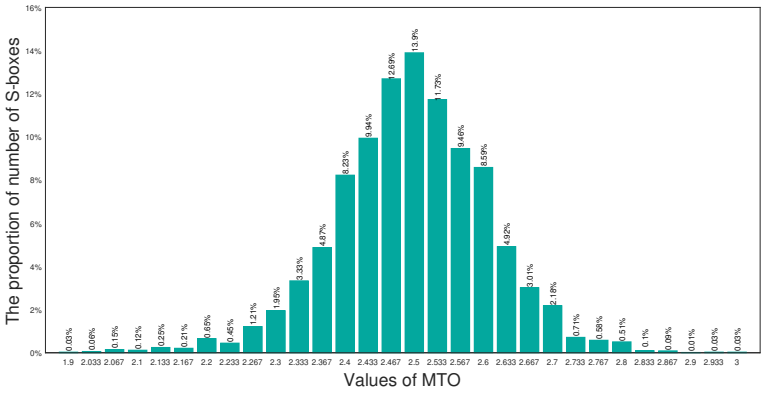


Fig. 12. Frequency distribution of MTO values of optimal S-boxes.

addition, the distributions of S-boxes with different TO, MTO and RTO values are also quite different. Therefore, the optimal S-boxes selected according to TO, MTO and RTO values should be quite different. Furthermore, it is noteworthy that MTO values of the optimal S-boxes range from 1.9 to 3, which is smaller than that of RTO (2.6 to 3.533). This also confirms that MTO underestimates the risk of S-boxes being subjected to DPA attacks.

D MTO_{min} values in the optimal classes

The MTO_{min} values for all 16 optimal classes' lower and upper bounds are given in Table 11, and the frequency distribution of all MTO_{min} values for all 16 optimal classes is shown in Fig. 13.

Table 11. MTO_{min} values of optimal S-boxes

S-box	$\#deg(S_b)$=3	MTO_{min} value		S-box	$\#deg(S_b)$=3	MTO_{min} value	
		Min	Max			Min	Max
S_0	15	1.600	2.267	S_8	12	1.333	2.533
S_1	15	1.567	2.400	S_9	12	1.333	2.533
S_2	15	1.567	2.400	S_{10}	12	1.333	2.533
S_3	15	1.567	2.367	S_{11}	12	1.333	2.533
S_4	15	1.567	2.333	S_{12}	12	1.333	2.367
S_5	15	1.567	2.333	S_{13}	12	1.333	2.367
S_5	15	1.600	2.300	S_{13}	12	1.333	2.333
S_7	15	1.567	2.367	S_{15}	12	1.333	2.400

It can be seen that there are 36 different MTO_{min} values for all optimal S-boxes, which are quite different from the results of RTO_{min}. And the distribu-

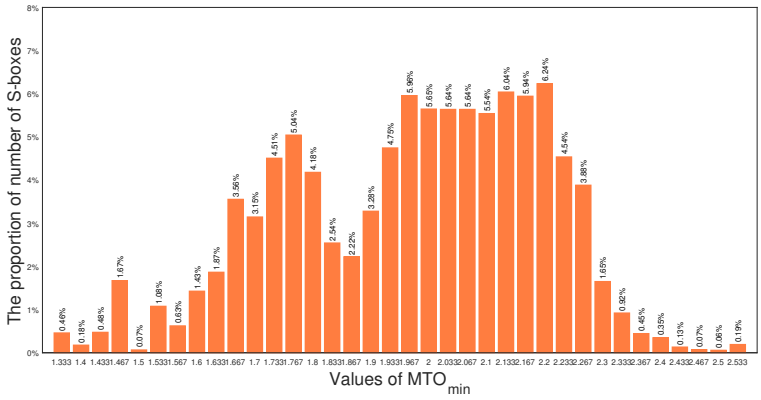


Fig. 13. Frequency distribution of MTO_{min} values of optimal S-boxes.

tions of S-boxes with different MTO_{min} and RTO_{min} values are also different. Similarly, by comparing the range of values for MTO_{min} and RTO_{min}, we can also draw the conclusion that MTO does underestimate the risk of S-boxes being subjected to DPA attacks.

E A lower bound of RTO(F) using Walsh spectrum

We present a lower bound of $\mathrm{RTO}(F)$ for a given $n \times m$ S-box F. The following lemma will be used to derive the bound.

Lemma 1. *Suppose e, f, g, h are Boolean functions of n-variables. Then*

$$\sum_{a \in \mathbb{F}_2^n} \mathcal{C}_{e,f}(a)\mathcal{C}_{g,h}(a) = \frac{1}{2^n} \sum_{a \in \mathbb{F}_2^n} W_e(a)W_f(a)W_g(a)W_h(a)\,.$$

The proof of **Lemma 1** can be found in reference [8].

Theorem 1. *For $F = (F_1, \cdots, F_m) : \mathbb{F}_2^n \to \mathbb{F}_2^m$, the value of RTO($F$) has the following lower bound*

$$\mathrm{m} - \frac{\sqrt{(2^n-1)\,m}}{2^{2n}-2^n} \left(\sum_{j=1}^{m} \left(\sum_{i=1}^{m} \sum_{a \in \mathbb{F}_2^{n*}} W_{F_i}^2(a) W_{F_j}^2(a) + 2 \sum_{1 \leqslant i < k \leqslant m} \sum_{a \in \mathbb{F}_2^{n*}} W_{F_i}(a) W_{F_j}^2(a) W_{F_k}(a) \right) \right)^{\frac{1}{2}}.$$

Proof. It is clear that $\mathrm{RTO(F)} \geqslant \mathrm{RTO(F,0)}$. So we calculate a lower bound of $\mathrm{RTO(F,0)}$. From Eq. (10) we get

$$\mathrm{RTO(F,0)} = \mathrm{m} - \frac{1}{2^{2\mathrm{n}} - 2^{\mathrm{n}}} \sum_{\mathrm{a} \in \mathbb{F}_2^{\mathrm{n}^*}} \left| \sum_{\mathrm{j}=1}^{\mathrm{m}} \sum_{\mathrm{i}=1}^{\mathrm{m}} \mathcal{C}_{\mathrm{F_i,F_j}}(\mathrm{a}) \right| .$$

Applying Cauchy-Schwarz inequality we get

$$\left(\sum_{j=1}^{m} \sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a) \right)^2 \leqslant m \sum_{j=1}^{m} \left(\sum_{i=1}^{m} \mathcal{C}_{F_i F_j}(a) \right)^2 .$$

Applying Cauchy-Schwarz inequality again, we get

$$\begin{aligned} \sum_{a \in \mathbb{F}_2^{n^*}} \left| \sum_{j=1}^{m} \sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a) \right| &\leqslant \left((2^n - 1) \sum_{a \in \mathbb{F}_2^{n^*}} m \sum_{j=1}^{m} \left(\sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a) \right)^2 \right)^{\frac{1}{2}} \\ &\leqslant \left((2^n - 1) \sum_{a \in \mathbb{F}_2^{n}} m \sum_{j=1}^{m} \left(\sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a) \right)^2 \right)^{\frac{1}{2}} \\ &= \left((2^n - 1)\, m \sum_{j=1}^{m} \sum_{a \in \mathbb{F}_2^{n}} \left(\sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a) \right)^2 \right)^{\frac{1}{2}} . \end{aligned} \tag{13}$$

Note that

$$\begin{aligned} \sum_{a \in \mathbb{F}_2^{n}} \left(\sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a) \right)^2 &= \sum_{a \in \mathbb{F}_2^{n}} \sum_{i=1}^{m} \mathcal{C}^2_{F_i,F_j}(a) + 2 \sum_{a \in \mathbb{F}_2^{n}} \sum_{1 \leqslant i < k \leqslant m} \mathcal{C}_{F_i,F_j}(a) \mathcal{C}_{F_k,F_j}(a) \\ &= \sum_{i=1}^{m} \sum_{a \in \mathbb{F}_2^{n}} \mathcal{C}^2_{F_i,F_j}(a) + 2 \sum_{1 \leqslant i < k \leqslant m} \sum_{a \in \mathbb{F}_2^{\mathrm{n}}} \mathcal{C}_{F_i,F_j}(a) \mathcal{C}_{F_k,F_j}(a) . \end{aligned} \tag{14}$$

Then applying Lemma 1,

$$\begin{aligned} \sum_{a \in \mathbb{F}_2^{n}} \left(\sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a) \right)^2 &= \sum_{i=1}^{m} \sum_{a \in \mathbb{F}_2^{n}} W^2_{F_i}(a) W^2_{F_j}(a) \\ &\quad + 2 \sum_{1 \leqslant i < k \leqslant m} \sum_{a \in \mathbb{F}_2^{n}} W_{F_i}(a) W^2_{F_j}(a) W_{F_k}(a) . \end{aligned}$$

Replacing this value of $\sum_{a \in \mathbb{F}_2^n} \left(\sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a) \right)^2$ in Eq. (13), an upper bound of $\sum_{a \in \mathbb{F}_2^{n^*}} | \sum_{j=1}^{m} \sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a)|$ is obtained. Then using this upper bound in Eq. (14), we get a lower bound of $\mathrm{RTO(F,0)}$ as follows

$$\mathrm{m} - \frac{\sqrt{(2^n-1)\,m}}{2^{2n}-2^n}\left(\sum_{j=1}^{m}\left(\sum_{i=1}^{m}\sum_{a\in\mathbb{F}_2^n} W_{F_i}^2(a)W_{F_j}^2(a) + 2\sum_{1\leqslant i<k\leqslant m}\sum_{a\in\mathbb{F}_2^n} W_{F_i}(a)W_{F_j}^2(a)W_{F_k}(a)\right)\right)^{\frac{1}{2}}.$$

Note that $\mathrm{RTO}(\mathrm{F},\beta)$ assumes that all the coordinate functions are balanced, therefore the above bound can be written as

$$\mathrm{m} - \frac{\sqrt{(2^n-1)\,m}}{2^{2n}-2^n}\left(\sum_{j=1}^{m}\left(\sum_{i=1}^{m}\sum_{a\in\mathbb{F}_2^{n*}} W_{F_i}^2(a)W_{F_j}^2(a) + 2\sum_{1\leqslant i<k\leqslant m}\sum_{a\in\mathbb{F}_2^{n*}} W_{F_i}(a)W_{F_j}^2(a)W_{F_k}(a)\right)\right)^{\frac{1}{2}}.$$

This serves as a lower bound of $\mathrm{RTO}(\mathrm{F})$.

References

1. Bevan, R., Knudsen, E.: Ways to enhance differential power analysis. In: International Conference on Information Security and Cryptology. pp. 327–342. Springer (2002)
2. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. Journal of CRYPTOLOGY **4**(1), 3–72 (1991)
3. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: International Workshop on Cryptographic Hardware and Embedded Systems. pp. 450–466. Springer (2007)
4. Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., et al.: PRINCE – a low-latency block cipher for pervasive computing applications. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 208–225. Springer (2012)
5. Carlet, C.: On highly nonlinear S-Boxes and their inability to thwart DPA attacks. In: International Conference on Cryptology in India. pp. 49–62. Springer (2005)
6. Carlet, C., Crama, Y., Hammer, P.L.: Boolean functions for cryptography and error correcting codes. Boolean models and methods in mathematics, computer science, and engineering **2**, 257–397 (2010)
7. Carlier, V., Chabanne, H., Dottax, E., Pelletier, H.: Electromagnetic side channels of an FPGA implementation of AES. In: CRYPTOLOGY EPRINT ARCHIVE, REPORT 2004/145. Citeseer (2004)

8. Chakraborty, K., Sarkar, S., Maitra, S., Mazumdar, B., Mukhopadhyay, D., Prouff, E.: Redefining the transparency order. Designs, Codes and Cryptography **82**(1-2), 95–115 (2017)
9. Chari, S., Jutla, C.S., Rao, J.R., Rohatgi, P.: Towards sound approaches to counteract power-analysis attacks. In: Annual International Cryptology Conference. pp. 398–412. Springer (1999)
10. Coron, J.S., Goubin, L.: On boolean and arithmetic masking against differential power analysis. In: International Workshop on Cryptographic Hardware and Embedded Systems. pp. 231–237. Springer (2000)
11. Dawson, M., Tavares, S.E.: An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks. In: Workshop on the Theory and Application of of Cryptographic Techniques. pp. 352–367. Springer (1991)
12. Doget, J., Prouff, E., Rivain, M., Standaert, F.X.: Univariate side channel attacks and leakage modeling. Journal of Cryptographic Engineering **1**(2), 123 (2011)
13. Evci, M.A., Kavut, S.: DPA resilience of rotation-symmetric S-boxes. In: International Workshop on Security. pp. 146–157. Springer (2014)
14. Fan, L., Zhou, Y., Feng, D.: A fast implementation of computing the transparency order of S-Boxes. In: 2008 The 9th International Conference for Young Computer Scientists. pp. 206–211. IEEE (2008)
15. Fei, Y., Luo, Q., Ding, A.A.: A statistical model for DPA with novel algorithmic confusion analysis. In: International Workshop on Cryptographic Hardware and Embedded Systems. pp. 233–250. Springer (2012)
16. Grosso, V., Leurent, G., Standaert, F.X., Varici, K., Durvaux, F., Gaspar, L., Kerckhof, S.: SCREAM & iSCREAM side-channel resistant authenticated encryption with masking. Submission to CAESAR (2014)
17. Guilley, S., Hoogvorst, P., Pacalet, R.: Differential power analysis model and some results. In: Smart Card Research and Advanced Applications Vi, pp. 127–142. Springer (2004)
18. Kavut, S., Baloğlu, S.: Classification of 6×6 S-boxes obtained by concatenation of RSSBs. In: International Workshop on Lightweight Cryptography for Security and Privacy. pp. 110–127. Springer (2016)
19. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Annual International Cryptology Conference. pp. 388–397. Springer (1999)
20. Kocher, P.C.: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Annual International Cryptology Conference. pp. 104–113. Springer (1996)
21. Leander, G., Poschmann, A.: On the classification of 4 bit S-Boxes. In: International Workshop on the Arithmetic of Finite Fields. pp. 159–176. Springer (2007)
22. Lim, C.H., Korkishko, T.: mCrypton – a lightweight block cipher for security of low-cost RFID tags and sensors. In: International Workshop on Information Security Applications. pp. 243–258. Springer (2005)
23. Mangard, S.: Hardware countermeasures against DPA – a statistical analysis of their effectiveness. In: Cryptographers Track at the RSA Conference. pp. 222–235. Springer (2004)
24. Mangard, S., Oswald, E., Popp, T.: Power analysis attacks: revealing the secrets of smart cards, vol. 31. Springer Science & Business Media (2008)
25. Matsui, M., Yamagishi, A.: A new method for known plaintext attack of FEAL cipher. In: Workshop on the Theory and Application of of Cryptographic Techniques. pp. 81–91. Springer (1992)

26. Mazumdar, B., Mukhopadhyay, D.: Construction of rotation symmetric S-Boxes with high nonlinearity and improved DPA resistivity. IEEE Transactions on Computers **66**(1), 59–72 (2016)
27. Mazumdar, B., Mukhopadhyay, D., Sengupta, I.: Design for security of block cipher S-Boxes to resist differential power attacks. In: 2012 25th International Conference on VLSI Design. pp. 113–118. IEEE (2012)
28. Mazumdar, B., Mukhopadhyay, D., Sengupta, I.: Constrained search for a class of good bijective S-Boxes with improved DPA resistivity. IEEE Transactions on Information Forensics and Security **8**(12), 2154–2163 (2013)
29. Mazumdar, B., Mukhopadhyay, D., Sengupta, I.: Design and implementation of rotation symmetric S-boxes with high nonlinearity and high DPA resilience. In: 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). pp. 87–92. IEEE (2013)
30. Messerges, T.S.: Power analysis attacks and countermeasures for cryptographic algorithms. University of Illinois at Chicago (2000)
31. Picek, S., Batina, L., Jakobovic, D.: Evolving DPA-resistant boolean functions. In: International Conference on Parallel Problem Solving from Nature. pp. 812–821. Springer (2014)
32. Picek, S., Ege, B., Batina, L., Jakobovic, D., Chmielewski, Ł., Golub, M.: On using genetic algorithms for intrinsic side-channel resistance: the case of AES S-Box. In: Proceedings of the First Workshop on Cryptography and Security in Computing Systems. pp. 13–18. ACM (2014)
33. Picek, S., Ege, B., Papagiannopoulos, K., Batina, L., Jakobović, D.: Optimality and beyond: The case of 4× 4 S-boxes. In: 2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). pp. 80–83. IEEE (2014)
34. Picek, S., Mazumdar, B., Mukhopadhyay, D., Batina, L.: Modified transparency order property: solution or just another attempt. In: International Conference on Security, Privacy, and Applied Cryptography Engineering. pp. 210–227. Springer (2015)
35. Picek, S., Papagiannopoulos, K., Ege, B., Batina, L., Jakobovic, D.: Confused by confusion: Systematic evaluation of DPA resistance of various S-boxes. In: International Conference in Cryptology in India. pp. 374–390. Springer (2014)
36. Picek, S., Yang, B., Mentens, N.: A search strategy to optimize the affine variant properties of S-Boxes. In: International Workshop on the Arithmetic of Finite Fields. pp. 208–223. Springer (2016)
37. Prouff, E.: DPA attacks and S-Boxes. In: International Workshop on Fast Software Encryption. pp. 424–441. Springer (2005)
38. Prouff, E., Rivain, M., Bevan, R.: Statistical analysis of second order differential power analysis. IEEE Transactions on computers **58**(6), 799–811 (2009)
39. Pub, N.F.: 197: Advanced encryption standard (AES). Federal information processing standards publication **197**(441), 0311 (2001)
40. Saarinen, M.J.O., Brumley, B.B.: STRIBOBr2:whirlbob, second round caesar algorithm tweak specification. CAESAR 2nd Round Candidate (2015)
41. Standaert, F.X., Piret, G., Rouvroy, G., Quisquater, J.J., Legat, J.D.: ICEBERG: an involutional cipher efficient for block encryption in reconfigurable hardware. In: International Workshop on Fast Software Encryption. pp. 279–298. Springer (2004)
42. Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., Verbauwhede, I.: RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. Science China Information Sciences **58**(12), 1–15 (2015)