SoK: Security Evaluation of SBox-Based Block Ciphers

Joelle Lim[1], Derrick Ng[1] and Ruth Ng[1,2]

[1] DSO National Laboratories, Singapore {lszemin,nweichen,niiyung}@dso.org.sg
[2] A*STAR

Abstract. Cryptanalysis of block ciphers is an active and important research area with an extensive volume of literature. For this work, we focus on SBox-based ciphers, as they are widely used and cover a large class of block ciphers. While there have been prior works that have consolidated attacks on block ciphers, they usually focus on describing and listing the attacks. Moreover, the methods for evaluating a cipher's security are often ad hoc, differing from cipher to cipher, as attacks and evaluation techniques are developed along the way. As such, we aim to organise the attack literature, as well as the work on security evaluation.

In this work, we present a systematization of cryptanalysis of SBox-based block ciphers focusing on three main areas: (1) Evaluation of block ciphers against standard cryptanalytic attacks; (2) Organisation and relationships between various attacks; (3) Comparison of the evaluation and attacks on existing ciphers.

Keywords: Security Evaluation · Block Ciphers · Substitution Box · Cryptanalysis

1 Introduction

In an increasingly data-driven world, the security and privacy of our data and communications is of vital importance. Block ciphers are widely used cryptographic primitives, which are building blocks that form the cornerstone of security schemes which protect this data. The block cipher as a cryptographic primitive has been popularized by the publication of the Data Encryption Standard (DES) by the United States National Bureau of Standards in 1977. Since then, there has been extensive study on block cipher design and the weaknesses they present. Block ciphers are commonly used today in algorithms such as the Advanced Encryption Standard (AES), which is prevalent in critical real-life applications everywhere.

The security evaluation of block ciphers is an active and important research area, with a copious amount of literature amassed on the topic to this day. Cryptanalysis describes this specific field of security evaluation in the context of studying the effectiveness of attacks against cipher designs. Modern cipher design has placed great importance on the resilience of their designs against known attacks. As such, much of the literature in this area has been concentrated on proving/arguing the security of ciphers against these attacks or demonstrating how these attacks may be applied to existing schemes (or part thereof).

This paper will present a systematization of cryptanalysis of SBox-based block ciphers focusing on three main areas: (1) Evaluation of block ciphers against standard cryptanalytic attacks; (2) Organisation and relationships between various attacks; and (3) Comparison of the evaluation and attacks on existing ciphers. More generally, we aim to compile, organize, and process the vast trove of knowledge on attacks of block ciphers, and present a high-level treatment of these attacks as applied to the security evaluation process of different ciphers. In particular, we will focus on SBox-based ciphers, as they are widely used and cover a large class of block ciphers.

ORGANIZATION. This paper proceeds as follows: Section 2 provides the readers with some background on block ciphers and attacks, and lays some groundwork necessary for the rest of the paper. Next, Section 3 consolidates the existing literature on SBox-based block cipher attacks and distills the essence of a varied list of cryptanalysis techniques, through the lens of the concrete security evaluation on an existing cipher. Then, Section 4 condenses the main properties of each attack to draw connections and perform classifications between different attacks. Finally, Section 5 provides a case study of the security evaluation processes adopted by designers of various popular SBox-based block ciphers, while Section 6 draws a conclusion to the paper.

OUR CONTRIBUTIONS. During the block cipher design process, there is a multitude of considerations to take into account when evaluating attacks. Due to the vast expense of literature available on block cipher cryptanalysis, it is easy to overlook certain aspects of attacks during security evaluation. This paper aims to amalgamate the information in this domain in a concise and easily-accessible manner, so that the reader may easily extract the information that they require to make informed choices when performing security evaluation.

The objectives of this work are as follows: first, to inform the reader on the current state of cryptanalysis techniques on SBox-based block ciphers, as they pertain to a security evaluation framework, enabling focus on techniques that will be useful in evaluating a specific cipher with its particular structure and characteristics and a given adversarial model; and second, to highlight the importance of a comprehensive security evaluation process. We hope to achieve these objectives with the following contributions:

- We revisit and formalize key notions associated to SBox-based block cipher. In particular, we revisit the definitions of Generalized Feistel Networks (GFN) and Substitution Permutation Networks (SPN), as well as the relationship between distinguisher-finding and key-recovery attacks. We formalize these precisely in the context of SBox-based block ciphers.

- We review fourteen cryptanalytic techniques from the literature that we determined to have been the most impactful toward modern cipher design. We take care to capture these distinct techniques using a novel and consistent syntax, thereby unifying these tools for use by future cipher designers. Specifically, we identify how each cryptanalytic technique can be used to build distinguishers, how these distinguishers can be extended to key recovery attacks, and what techniques exist to protect ciphers against such attacks.

- To help contextualize cryptanalytic techniques for those new to the area, we draw connections between known cryptanalytic techniques, including the fourteen major ones presented above. We also revisit the classification of these attacks with refreshed definitions of structural, statistical and algebraic definitions.

- Finally, we provide a novel case study of popular schemes that emerged from cryptographic competitions. In particular, we compare the security assurances given by the schemes' designers (with respect to our highlighted cryptanalysis techniques) to attacks that have emerged in the 20+ years that have passed. From this, we gain novel insight into how security evaluations evolve over time, and draw conclusions that could be of interest to future research, cipher designers and cryptographic competitions.

2 Background

In this section, we provide background on SBox-based block ciphers, including GFN and SPN (with variants). We also give an overview on cryptanalytic techniques and attack models.

Block ciphers, SBoxes. A block cipher is a method of encryption where plaintexts are encrypted in n-bit blocks to n-bit ciphertext blocks. Given key k, a block cipher specifies an encryption algorithm E_k and a decryption algorithm D_k, such that $D_k \circ E_k$ is the identity on n-bit plaintexts [VTJ14].

An SBox (Substitution-box) is an b_1-bit to b_2-bit function that typically has a non-linear algebraic expression and is used to inject non-linearity into a cipher system. There has been a great deal of research performed on constructing good SBoxes, and the impact of SBoxes on cryptanalysis is fairly well studied. As such, many ciphers are constructed with SBoxes as their underlying backbone. In our discourse, we only consider ciphers that derive their non-linearity from SBoxes.

GFNs. Feistel networks form the basis of a widely used design philosophy to design block ciphers by the modern cryptographic community. The classical vanilla Feistel structure (as deployed in DES) works as follows: Given an n-bit string, the Feistel structure divides it into two halves L (left) and R (right) called branches. During each round, a (non-linear) round function $F(R, k)$ is applied to the right branch and the result is XORed with the left half in the operation $\phi : (L, R) \leftarrow (R, L \oplus F(R, k))$, where k is the round subkey produced by the key scheduling algorithm. The branch positions are then swapped before the next round. More generally, the n-bit string may be divided into smaller strings instead of halves, and a branch permutation is applied to swap their branches around [VTJ14].

A key feature of the Feistel structure is the similarity between the encryption and decryption processes. In particular, the classical Feistel structure as constructed above provides invertible transformations independently of whether the round function F is invertible or not. Additionally, Feistel structures also allow for efficient spreading of the diffusion (changing one bit affects many bits) and confusion (each bit depends on many bits) properties of the round function between branches. In particular, we can construct a Pseudo-Random Permutation (PRP) from just 3 rounds of a classical 2-branch balanced Feistel network [LR88]. This allows a designer to fully concentrate on the security properties of the round function when making security evaluations [Nyb96]. Note that while the round function can be constructed in a myriad of ways, we are only interested in SBox-based constructions here.

We can further generalize the classical notion of a Feistel structure, by considering similar structures which spread the diffusion and confusion properties of the round functions across branches in different ways. For instance, certain ciphers such as MISTY1 apply the round function to the actual branches via the round operation $\phi : (L, R) \leftarrow (R, F(L, k) \oplus R)$ [Mat97].

In order to encapsulate all these variations, we look at a broader class of ciphers known as Generalized Feistel Networks (GFN). These include: unbalanced Feistel networks with expanding or contracting round functions; alternating Feistel networks, where the rounds alternate between contracting and expanding steps; nested Feistel networks where the round functions are themselves Feistel networks; type-1, type-2, and type-3 Feistel networks, each of which uses 1, 2, or 3 n-bit to n-bit round functions respectively to create a kn-bit block cipher for some $k \geq 2$; and numeric variants of any of the above, where one enciphers numbers in $\mathbb{Z}_N$, for some $N \in \mathbb{N}$, instead of enciphering binary strings. Some examples of block ciphers that use generalized Feistel networks include Skipjack (an unbalanced Feistel network), BEAR/LION (alternating), MISTY1 (nested), CAST-256 (type-1), CLEFIA (type-2), and MARS (type-3) [HR10].

SPNs. Another popular design philosophy for block ciphers is the Substitution-Permutation Networks (SPN) structure. While exceptions (such as KATAN/KTANTAN [DDK09]) exist, a vast majority of block ciphers that are not GFN are either SPN or a variant of it. SPN derive their security by composing several rounds of interleaving substitutions and

Table 1: Classification of various notable SBox based ciphers by structure.

GFN Ciphers			**Non-GFN Ciphers**		
CLEFIA	KASUMI	DES	**AES**	SASAS	ARIA
SKIPJACK	**Camellia**	LBlock	**Serpent**	SKINNY	SAFER
LOKI	**MISTY1**	GDES	3-WAY	KHAZAD	KLEIN
GOST	TripleDES	Biham-DES	LED	LowMC	CRYPTON
CAST	DES-X	NewDES	PRINTCIPHER	SQUARE	**Hierocrypt**
Blowfish	TWINE	Piccolo	HADES	PRESENT	NOEKEON
FEAL	**Twofish**	WARP	**SC2000**	GIFT	
	MARS				

permutations. Although weak on its own, a line of substitutions followed by a permutation has good "mixing" properties: substitutions (often via SBoxes) add to local confusion and permutations diffuse the local confusion to the more distant sub-blocks, triggering an avalanche effect over multiple rounds. Some variants of SPN use linear or affine mappings instead of bit permutations to achieve better diffusion in fewer iterations. Such networks are called Substitution-Linear Networks (SLN) or Substitution-Affine Networks (SAN) respectively. Rijndael/AES is a prominent example of an SLN cipher. In this work, for brevity, we will refer to all SPN/SLN/SAN schemes collectively as "SPNs".

To concretize these definitions, we collected a list of notable SBox-based ciphers in the literature. While we do not claim that this list is exhaustive, we believe it contains all schemes with substantial visibility (i.e. citations). We note that every scheme on our list was either a GFN or SPN, as detailed in Table 1.

In Section 2 we will give an overview of distinguishers and attacks on these SBox-based ciphers (from either one or both of these classes). In Section 5, we do a detailed literature review of nine of these schemes, which are **bolded** in Table 1.

ATTACKER MODELS. In this paper, we will be providing an exposition of the various attacks applied on block ciphers. Before we proceed, we would like to first make a brief comment on distinguisher-finding attacks and key recovery attacks. In most cases, the tools developed by the various cryptanalytic techniques do not allow attackers to recover the key directly, but instead allow them to find a $m-$round distinguisher. These distinguishers are often based on a certain property or characteristic constructed from the attack, and enable attackers to distinguish a correct instantiation of the attacked cipher with the correct key, from a random function or permutation with a higher than random probability.

Distinguishers may be extended to key-recovery attacks through an appropriate application of the distinguisher and a good choice of PT-CT pairs to propagate our desired characteristic so that the conditions of the distinguisher can be met. In particular, for the Differential Cryptanalysis (DC), Linear Cryptanalysis (LC), Zero-Correlation Linear Cryptanalysis (ZCLC), Impossible Differential Cryptanalysis (IDC) and Integral attacks, the extension from a distinguisher attack to a key-recovery attack typically works as follows: Suppose our distinguisher attack indicates that a set of input-output pairs exhibits a certain characteristic that can be distinghished from random permutation through a certain number of rounds, which we shall label as the core rounds. Then, we can add additional rounds before and after the core rounds, and select appropriate PT-CT pairs that will propagate through the additional rounds to a set of input-output pairs to the core rounds that exhibit our desired characteristic if the subkey guess to these additional rounds is correct. We can then identify, and hence recover, the correct subkey by observing the subkey guess for which the distinguishing property holds. This set of input-output pairs to the core rounds differs from attack to attack.

3 Overview of Cryptanalytic Techniques

In this section we will provide a short discourse on several attack techniques, mainly on how they may be applied as distinguisher attacks. This is because our focus is on security evaluation, where one aims to ensure that no distinguishers of sufficiently high probability exist for r rounds. To this end, we will highlight the techniques used to find longest possible distinguishers and estimate their probabilities. These include the main algorithms used, as well as mixed-integer linear programming (MILP), SAT and constraint programming approaches, which have recently gained popularity. We have included in Table 3 a brief description of the distinguishers and security evaluation techniques.

In all the subsections that follow, we will use X and Y (and subscripted versions of these) to denote intermediate cipher states. In general, X will refer to a state closer (in terms of rounds) to the plaintext, while Y is closer to the ciphertext. The states X and Y are usually a few rounds away from the the plaintext and ciphertext respectively, since key recovery attack extends the distinguisher.

DIFFERENTIAL CRYPTANALYSIS Differential cryptanalysis, first published in [BS91], is a chosen plaintext attack that exploits predictable difference propagations, i.e. $\Delta X \rightarrow \Delta Y$ for r rounds with higher than random probability. Here, ΔX refers to a known fixed difference pattern for the cipher state X. For later sections, we may specify the difference pattern as $\Delta \rightarrow \Delta^*$ or $\nabla \rightarrow \nabla^*$ to illustrate the attacks.

Observe that the difference propagation is deterministic for linear portions of the cipher but probabilistic for the SBox portions. An approach to evaluate cipher's security against differential cryptanalysis approximates the probability of a differential path by taking the product of the differential characteristic probability of the active SBoxes [Dae95]. Hence evaluating the security reduces to finding a differential path with the minimal number of active SBoxes. The AES designers used this method, showing that since the minimum number of active SBoxes in any 4-round differential trail is 25 and the SBox differential probability is 2^{-6}, the maximum differential probability of $2^{-6\times 25} = 2^{-150}$ for any 4-round differential trail [DR03].

The first generic algorithm for differential path searching is Matsui's branch-and-bound search algorithm [Mat95]. This breadth-first search was later improved using search patterns [OMA95], using a pre-search [AKM97] and with various other techniques in [BZL15, JZD21]. MILP has also been used to construct automatic differential (and linear) path searches including work in [WW11, MWGP12].

In Sony's original specification documentation on CLEFIA, a computer search yielded a lower bound of 28 active SBoxes for any 12-round differential trail [Son07]. Together with the maximal SBox differential probability of $2^{-4.67}$, they showed that the maximal differential probability for 12 rounds is $2^{-4.67\times 28} = 2^{-130.76}$. Wu–Wang's paper [WW11] had a more pessimistic result, with a lower bound of 24 active SBoxes for any 13-round differential trail in CLEFIA.

In truncated differential cryptanalysis, distinguishers are $\Delta X \rightarrow \Delta Y$, where the explicit word or byte differences are not specified, and only stated as zero or nonzero difference. This relaxation of the differential attack was first introduced in [Knu95] and used in meet-in-the-middle attacks against CLEFIA and Camellia [LJWD15]. The concept of truncated differentials has been applied to differential-linear cryptanalysis as well as in the construction of impossible differential distinguishers.

LINEAR CRYPTANALYSIS The linear cryptanalysis attack, first studied in [MY93], is a known plaintext attack that uses linear approximations, i.e. equations of the form $\alpha \cdot X = \beta \cdot Y$ (for some vectors (α, β) called masks) which hold with biased probability greater than $\frac{1}{2}$. One can linearly approximate the SBoxes to get the bias for a linear path.

To concatenate the probabilities of multiple such linear approximations, Matsui introduces the piling-up lemma [Mat94], which assumes that the approximations are independent.

Table 2: Attacks and Corresponding Security Evaluation Methods

Attack type	Distinguisher structure	Method of Security Evaluation
Differential (DC)	$\Delta X \rightarrow \Delta Y$ with high probability	Use duality between DC and LC. Matsui's path search [Mat95] and improvements [OMA95, AKM97, BZL15, JZD21]. MILP tools [MWGP12, WW11]
Linear (LC)	$\alpha \cdot X = \beta \cdot Y$ with high probability	
Impossible Differential (IDC)	$\Delta X \rightarrow \Delta Y$ with zero probability	Use duality between IDC and ZCLC. Miss-in-the-middle methods ($\mathcal{U}$, UID), Wu–Wang [WW12], MILP [CJF+16, ST16] and CP [SGL+17] tools
Zero Correlation Linear (ZCLC)	$\alpha \cdot X = \beta \cdot Y$ with probability 1/2	
Differential-Linear (DLC)	Cipher has two components $E = E_1 \circ E_0$ E_0 with $\Delta X_0 \rightarrow \Delta X_1$ E_1 with $\alpha \cdot X_1 = \beta \cdot X_2$ with high probabilities	Combine longest differential and linear paths, estimate differential-linear bias based on independence assumptions [BDK02a, LGZL10, Lu12] or estimate bias from closed form [BLN15]
Boomerang	Cipher has two components $E = E_1 \circ E_0$ E_0 with $\Delta X_0 \rightarrow \Delta X_1$ ${E_1}^{-1}$ with $\Delta Y_0 \rightarrow \Delta Y_1$ with high probabilities	Combine long differential paths with high probability. Use Boomerang Connectivity Table [CHP+18, BHL+20], or Boomerang Difference Table [WP19] to find trails and probability or a method by Song et al. [SQH19] MILP, SMT/SAT and CP tools [DDV20, HBS20]
Higher Order Differential	$\Delta^d X \rightarrow \Delta^d Y$ with high probability	Heuristic approach, give upper bound on degree of the polynomial describing the cipher after r rounds [BCD10]
Related Key Differential	$(\Delta X, \Delta K) \rightarrow \Delta Y$ with high probability	Use DC method on key schedule (upper bound) [Son07] or estimate probability [CZK+11]
Related Key Boomerang	Cipher has two components $E = E_1 \circ E_0$ E_0 with $(\Delta X_0, \Delta K) \rightarrow \Delta X_1$ ${E_1}^{-1}$ with $(\Delta Y_0, \Delta K) \rightarrow \Delta Y_1$ with high probabilities	Combine differential paths on key schedule [Son07] or estimate probability [CZK+11]
Integral	Known pattern in the X leading to known patterns in Y (patterns: active, zero or balanced)	Tracing the division property [Tod15b] and bit-based variant [TM16] MILP [XZBL16], SAT [EKKT19], CP [SGL+17] tools
Slide	Cipher E is composed of functions $F(X, K)$, X, X' such that $F(X, K) = X'$	Heuristic evaluation of key schedule uniformity e.g. independent round constants provide security [Son07]
Interpolation or other algebraic attacks	Various algebraic relations between X and Y	Heuristic approach, estimate the number of equations and terms [CP02, Son07], or algorithm for linear sum security [Aok00]
Meet in the Middle (MiTM)	Cipher has three components $E = E_2 \circ E_1 \circ E_0$ Distinguisher on E_1 only affected by subkeys in E_0, E_2	Ad-hoc approaches using the distinguishers above, or search tools [LWWZ14, DF16, SSD+18]

It was also observed that for a given linear relation, there could be multiple possible intermediate linear paths, combining to give a higher linear probability. Nyberg introduced the term linear hull to refer to the set of all such linear trails [Nyb95]. Despite these, the independence assumption appears reasonable for many ciphers, and when one linear trail has a high bias, it tends to dominate the linear hull [Hey02].

Hence, security evaluations tend to involve finding a linear trail with a minimal number of active SBoxes and computing the linear probability by the piling-up lemma. For example, for CLEFIA, there are at least 30 active SBoxes for any 12-round linear path and the maximum linear probability of the SBoxes is $2^{-4.38}$, yielding a maximal linear cryptanalysis probability of $2^{-4.38 \times 30} = 2^{-131.40}$ for 12 rounds [Son07].

Biham observed that linear and differential cryptanalysis are structurally similar [Bih95]. For example, they have similar security estimation methods. Matsui followed up on this correspondence, observing that a path $a \to b$ is a differential trail of a cipher if and only if it is a linear hull of the dual structure, where the dual cipher is constructed by observing that an XOR operation after an F function and a three-forked branch before the F function are mutually dual [Mat95].

To account for differential and linear cryptanalytic techniques in cipher design, two approaches were considered. The wide trail strategy [DR01], which was used in AES design, aims to design the round transformations such that there are no trails with few active SBoxes. Another method, decorrelation [Vau03], constructs ciphers from primitives with sufficient pseudorandomness, using this to compute that the maximal differential and linear probabilities and prove that are too low to mount a linear or differential attack. However, COCONUT, constructed via decorrelation was shown to be vulnerable to some attacks where differential (and linear) distinguishers were used in combination [Wag99, BDK02a].

IMPOSSIBLE DIFFERENTIAL CRYPTANALYSIS Impossible differential attacks were first used by Knudsen [Knu98] and generalised and named in [BBS99]. These attacks use impossible difference propagations, i.e. $\Delta X \to \Delta Y$ with zero probability as a distinguisher. The general attack strategy is as follows. Firstly select many structures of chosen plaintexts and sieve the pairs satisfying the required output differences. Secondly, for each sieved pair, discard the wrong subkeys which cause the partial encryption and decryption to match the impossible differential. Lastly, analyse enough pairs and sieve the correct subkey.

Some work to construct impossible distinguishers include the miss-in-the-middle $\mathcal{U}$ method [KHS+03] and its generalisation, the UID method [LWLG09]. In these approaches, the cipher functions are modelled as a matrix applied on vectors to study the difference propagation. They consider four cases: zero difference, nonzero fixed difference, nonzero unspecified difference and unknown difference. In particular, they are built from truncated differentials.

However, the miss-in-the-middle structure does not account for impossible differentials with information feedback. These are structure where there is no contradiction in the middle matching point, instead, the matching point forces some constraints on other parts of the cipher, which lead to a contradiction. Many known impossible differential distinguishers are of this form such as those on 9-rounds CLEFIA [TTS+08b]. To account for these, Wu–Wang use a more generic approach [WW12], which was proven to find all impossible differentials of a cipher that are independent of the SBox choices [SLR+15]. MILP tools [CJF+16, ST16] and constraint programming [SGL+17] have also been used to find impossible differential distinguishers.

ZERO CORRELATION LINEAR CRYPTANALYSIS Zero correlation linear cryptanalysis, based on linear approximations with probability $\frac{1}{2}$, i.e. unbiased or with zero correlation, is an extension of linear cryptanalysis first proposed by [BR11] and later extended to include multiple zero correlation distinguishers [BW12].

The correlation between two functions f, g is $C(f, g) = 2(Pr(f(x) = g(x)) - 1$, i.e. it measures the likelihood of two functions matching each other. In the cryptanalytic setting, we consider $C(\alpha \cdot X, \beta \cdot Y)$, where (α, β) is the mask. For any non-trivial linear approximation (α, β) of an n-bit permutation, the correlation value can be evaluated with 2^{n-1} input-output pairs (x, y) [BR11]. This is used to evaluate a key guess, as in the attack launched in [BGW⁺14].

In the linear cryptanalysis case, the correlation is as high as possible, since the masking is chosen so that $Pr(\alpha \cdot X = \beta \cdot Y)$ is high. With this in mind, zero correlation linear cryptanalysis can be viewed as the linear counterpart of impossible differential cryptanalysis. Bogdanov–Rijmen suggested a relationship between the impossible differential and zero correlation linear distinguishers. It was later shown that a zero correlation linear hull of a block cipher is an impossible differential characteristic of the corresponding dual cipher and vice versa [SLR⁺15]. This allows an attacker to run the same distinguisher-finding tools as for impossible differential distinguishers.

Square, Saturation, Integral Cryptanalysis Square attacks are based on the dedicated attack constructed on SQUARE [DKR97], which was later extended to other ciphers processing data blocks in fixed-size words at a time [NBP⁺01]. This included the first notion of the balanced property, when the words in a particular position over the set of plaintexts sum to zero. Square attacks were used against Hierocrypt [BRN⁺02] as well as AES-192 and AES-256 [GM00]. A variant of the square attack, the saturation attack, was introduced in [Luc02]. An improvement to the original square attacks includes the partial sum technique [FKL⁺01].

Square and saturation attacks are precursors of integral cryptanalysis [KW02]. In an integral attack, an attacker tries to predict the properties of the sum of all ciphertext values, i.e. whether words in a certain position are all the same (constant) or all different (active) or the words sum to a known specific value, e.g. zero (balanced). To construct integral distinguishers, these properties were further generalised to the division property which can be traced based on the cipher operations [Tod15b]. A variant of the division property, specifically an extension to the bit-based case, was constructed in [TM16]. Using the division property, one can use MILP [XZBL16], SAT solvers [EKKT19] or constraint programming [SGL⁺17] to automate the construction of integral distinguishers.

Integral distinguishers can be derived from impossible differentials and zero-correlation linear differentials. In particular, both r-round ZCLDs and IDs yield r-round integral distinguishers [SLR⁺15]. This was used on CLEFIA [YC16]. Moreover, for CLEFIA, an 8-round distinguisher was first proposed by the designers [Son07] and used to construct an 11-round saturation attack [WW08]. Subsequently, 9-round distinguishers were found in [LWZ12, YC16] and used in attacks of up to 15 rounds.

Differential-Linear Cryptanalysis The differential-linear attack was introduced by Langford–Hellman as a method to combine differential and linear attacks [LH94]. A notable differential-linear attack was on full round COCONUT98, in spite of its provable security claim on both differential and linear security [BDK02a]. Suppose that the cipher (or sub-cipher) E can be decomposed as $E = E_1 \circ E_0$, where there is a differential (or truncated) characteristic on E_0 given by $\Delta X_0 \to \Delta X_1$ (with a specified difference pattern $\Delta \to \Delta^*$) and a linear approximation of E_1 given by $\alpha \cdot X_1 = \beta \cdot X_2$, both of high probabilities.

Consider an pair of plaintexts $(X_0, X_0 \oplus \Delta)$. Applying E_0 maps the plaintexts to the same round state as X_1, while applying E maps them to the same round state as X_2. Hence we can apply the linear correlation and obtain $\alpha \cdot E_0(X_0) = \beta \cdot E(X_0)$ and $\alpha \cdot E_0(X_0 \oplus \Delta) = \beta \cdot E(X_0 \oplus \Delta)$ with high probabilities. Then taking the XOR of these equations and using the differential characteristic, with high probability we get

$$\alpha \cdot \Delta^* = \alpha \cdot (E_0(X_0) \oplus E_0(X_0 \oplus \Delta)) = \beta \cdot (E(X_0) \oplus E(X_0 \oplus \Delta))$$

The bias that this linear approximation holds, called the differential-linear bias, has been studied heuristically by Biham et al. [BDK02a], Liu et al. [LGZL10] and Lu [Lu12] under different independence assumptions. It is not clear whether these assumptions hold in general - Biham et al. assume that the distribution of $\beta \cdot (E(X_0))$ and $\beta \cdot E(X_0 \oplus \Delta)$ is independent and uniformly distributed, but Lu shows that this might not be the case [Lu12]. Further work by Blondeau et al. used a relation between linear and differential cryptanalysis to give a closed form for the bias, only under the assumption that two sub-ciphers are independent [BLN15]. However, evaluating this form is computationally intensive.

RECTANGLE AND BOOMERANG ATTACKS The boomerang attack was discovered by Wagner as an extension of differential cryptanalysis [Wag99]. It involves decomposing the cipher E into two components, i.e. $E = E_1 \circ E_0$ and using two unrelated differential characteristics (or truncated differentials), $\Delta \to \Delta^*$ for E_0 and $\nabla \to \nabla^*$ for E_1^{-1}, with high probabilities (rather than one long differential with a low probability). A boomerang distinguisher is a quartet of plaintext-ciphertext pairs, such that P, P', Q, Q' and corresponding ciphertexts C, C', D, D' satisfy the following:

- The pairs (P, P') and (Q, Q') each satisfy $\Delta \to \Delta^*$ after applying E_0
- The pairs (C, D) and (C', D') each satisfy $\nabla \to \nabla^*$ after applying E_1^{-1}

Wagner used this technique to construct longer distinguishers, breaking the cipher COCONUT, which was constructed to be provably secure against differential attacks [Vau03]. A disadvantage is that the boomerang attack requires rather strong conditions - both adaptively chosen plaintext and adaptively chosen ciphertext queries are needed to run the attack.

Following this, there have been several extensions to the boomerang attack. The amplified boomerang attack removes the chosen-ciphertext condition at a cost of more chosen-plaintext queries [KKS01], while the rectangle attack builds on the amplified attack, using multiple boomerang distinguishers, where the differences in the center of the cipher are not fixed, as long as they sum to zero [BDK01]. Dunkelman et al. introduced the sandwich attack, where a short middle layer is added so the cipher is decomposed as $E_1 \circ E_m \circ E_0$ [DKS14]. A variant of boomerang attack, which also requires adaptively chosen plaintexts and ciphertexts is the yoyo attack. It was first introduced in [BBD+99] and later extended to SPN structures and AES in [RBH17].

In Wagner's original attack, the two differentials are assumed to be independent. However, their dependencies have shown to either aid the attack (boomerang switches [Vau03] , [BK09]) or reduce its effectiveness [Mur11]. Some tools constructed to account for these dependencies include the boomerang connectivity table [CHP+18, BHL+20], the boomerang difference table [WP19], a method by Song et al. to determine the choice of middle length [SQH19], as well as some SMT/SAT, MILP and CP solvers [DDV20, HBS20]. More recently, Kidmose–Tiessen have conducted a theoretical analysis of the probabilities of these distinguishers [KT22].

RELATED KEY DIFFERENTIAL CRYPTANALYSIS Related key attacks were first studied by Biham [Bih94] and later extended using differential cryptanalysis by Kelsey et al. [KSW96]. Related key differential cryptanalysis is an extension of differential cryptanalysis where the key difference is known or chosen by the attacker, and is part of the differential characteristic. To launch the attack, one attempts to find a triplet of differences in the plaintext, ciphertext and key i.e. $(\Delta X, \Delta K) \to \Delta Y$ that holds with high probability.

Related key differential cryptanalysis has been used to construct a full attack on AES-256 by exploiting the key schedule's slow diffusion and local collisions from matching differential properties between the key schedule and the cipher rounds [BKN09]. The attack has a 2^{131} time, 2^{65} memory complexity and requires 2^{35} related keys on average.

In [CZK+11], Choy et al. present a framework to evaluate a block cipher's security against related key differential and boomerang attacks. They showed that security against these attacks follows if the number of active SBoxes in a differential characteristic of the key schedule and the number of active SBoxes in the differential characteristic of the main cipher, conditioned on subkey differences from the key schedule, is large enough. Specifically, by Bayes' theorem they have the following:

$$Pr(\Delta P, \Delta K \to \Delta C) = Pr(\Delta K \to \Delta K_0, \ldots \Delta K_m) \cdot Pr(\Delta P \to \Delta C | \Delta K \to \Delta K_0, \ldots \Delta K_m)$$

where the first term considers the key schedule differential characteristic and K_i are the subkeys, K is the key, and P, C are the plaintext and ciphertext respectively. The authors denote the first probability in the product as p_k and the second as $p_{c|k}$. In practice, it is often sufficient to consider the p_k component. For example, for CLEFIA, the designers evaluated its security against the related key differential attack by consider the differential characteristic of the key schedule [Son07]. Since it has the same round structure as the main cipher, the same differential probability computed for DC was used to show CLEFIA's security in the related-key setting.

RELATED KEY BOOMERANG AND RECTANGLE ATTACKS The first mention of related key rectangle attacks was by Kim et al. in [KKH+04], where the authors combine a differential with a related key differential. Biham et al. and Hong et al. concurrently revised this notion to combine two related key differentials in the attacks[BDK05b, HKLP05]. This method of cryptanalysis was also used by Biryukov–Khovratovich to attack full AES-192 and AES-256 [BK09].

In related key boomerang or rectangle attacks, the cipher E is decomposed into two components, $E = E_1 \circ E_0$ and a related-key differential is applied on each sub-cipher. Leveraging on the boomerang attack style, the related key variant is able to use shorter related-key differentials for the similar length distinguisher, so there is potentially less diffusion of differences in the subkeys. However, the attack also inherits the issues faced in estimating complexity for the boomerang attack. Kim et al. conducted experimental verification and more rigorous analysis of the related key boomerang and rectangle attacks, observing that while the results are on average close to theoretical, there is high variance in the exact probability, i.e. works well for some keys but fails for others [KHP+12].

For the first related key differential, we let p_k refer to the key schedule differential characteristic probability and $p_{c|k}$ refer to the conditional probability. We define q_k and $q_{c|k}$ in the same way for the second related key differential. Then Choy et al. show in [CZK+11] that:

- the cipher is secure against a related key boomerang attack if the probability $(p_k q_k)^2 (p_{c|k} q_{c|k})^2$ is less than the inverse of the keyspace
- that there will be insufficient plaintexts to launch the attack if $(p_{c|k} q_{c|k})^2$ is less than the inverse of the plaintext space

In practice, one may take an upper bound: in [Son07], the designers evaluated security by showing that $(p_k q_k)^2$ is less than the inverse of the keyspace.

SLIDE ATTACKS Slide attacks were first used in an unpublished manuscript in 1998, which was later made available in [Saa19], to recover the secret SBoxes in GOST. Officially introduced by Biryukov—Wagner [BW99], it is the first attack that is often independent of the number of rounds. The attack works if the cipher can be decomposed into a product of identical permutation functions $F(x, k)$, where k is the fixed secret key. The F function may consist of more than one cipher round, but the key k should be "easy" to extract given two plaintext-ciphertext pairs $F(x_1, k)$ and $F(x_2, k)$.

To run the attack, the attacker first finds plaintexts P, P' such that $F(P, k) = P'$, then the corresponding ciphertexts C, C' also satisfy $F(C, k) = C'$. The set (P, C), (P', C') is called a slid pair and can be used by the property above to extract the key k. Slide attacks require some periodicity or self-similarity in the round keys.

Improvements to the slide attacks include two variants: sliding with a twist and complementation slide [BW00], which extend the attack on new classes of ciphers (Feistel ciphers with two round self-similarity, and four round self-similarity if these variants are combined). A variant in [BDK07] finds slid pairs more efficiently. Another attack that depends on self-similarity on the rounds is the reflection attack [Kar07, DDKS15]. Slide attacks have also been used in combination with algebraic attacks [CBW08].

Since CLEFIA uses round constants independent of each round, the designers argue that it does not have a self-similarity property that can be exploited to construct a slide attack [Son07].

HIGHER ORDER DIFFERENTIAL CRYPTANALYSIS Higher order differential cryptanalysis generalises differential cryptanalysis, exploiting higher order differentials over several rounds that hold with high probability. We will denote a d-th order differential as $\Delta^d X \to \Delta^d Y$. This attack was first introduced by Lai in [Lai94] and further developed by Knudsen in [Knu95].

In particular, observe that if the algebraic degree of the ciphertext (or the round state a few rounds before) as a function of the plaintext is d, the d-th order differential over is a constant and can be used as a distinguisher in a higher order differential attack. Ciphers such as a reduced version of MISTY1 were shown to be vulnerable against higher order differential distinguishers, despite being secure against differential attacks [CV02].

It is difficult to analytically ensure security against higher order differential attacks, i.e. ensure that no high probability higher order differentials exist. Heuristically, a high algebraic degree for several rounds for the cipher makes it unlikely that a higher order differential attack will work. For a d-th order differential, 2^{d+1} plaintexts are needed to compute the derivative, so the complexity of the attack is higher with a higher order.

A trivial bound for the algebraic degree of r rounds is $(\deg F)^r$, where F is the round function, however, the degree of the composition of F might grow much slower. The first improvement of this bound was provided by Canteaut–Videau [CV02] and later by Boura et al. [BCD10]. More specifically, given a cipher round function F (on state size n bits) and any function G also on n bits, Boura et al. showed that

$$\deg(G \circ F) \leq n - (n - \deg G)/(b-1)$$

where b is the bitsize of the SBoxes. This gives a heuristic upper bound on the degree of F^r.

INTERPOLATION AND CUBE ATTACKS The main idea behind interpolation attacks is that the ciphertext can be expressed as a polynomial in terms of the plaintext. Given enough plaintext/ciphertext pairs, one can use the Lagrange interpolation formula to recover the coefficients of this polynomial. After constructing the polynomial of the ciphertext decrypted by one round, one more plaintext ciphertext pair is used to verify the guess. For the correct last-round key, the plaintext and ciphertext decrypted one round would also satisfy the polynomial constructed.

In the first work on interpolation attack by Jakobsen—Knudsen in [JK97], this attack was applied to a variant of SHARK which was provably secure against differential and linear cryptanalysis. Interpolation attack was shown to work well against ciphers with low algebraic degree. Improvements on the interpolation attacks include using the Moebius transform to reduce the time complexity [DLMW15], removing the requirement to brute force the last-round key and interpolation of only one coefficient in the polynomial to reduce the memory requirement [LP19]. The low/constant memory attack is restricted to some key-alternating and Feistel network structures. Modifications to the original attack include [KID01], where Kurosawa et al. observed that Jakobsen—Knudsen underestimated the number of plaintext/ciphertext pairs needed, i.e. the key found might not be unique.

They used Rabin's root finding method to find the set of equivalent keys in this case and derived an upper bound for the number of equivalent keys in the chosen plaintext case.

To analyse the attack effectiveness, Youssef—Gong considered how the degree of the interpolated polynomial varied depending on the choice of the irreducible finite field polynomial used as well as if the linear transformation were applied on input or output bits of the SBoxes (or the round function) [YG01]. Aoki generalised this attack to the linear sum attack and developed an algorithm to evaluate the security of byte-oriented ciphers under this attack [Aok00]. Aoki also showed that security against the linear sum attack implies security against higher order differential attacks.

Cube attacks, first introduced in [DS08b], involve setting up and solving a linear system of polynomials in $GF(2)$ describing the cipher. It has a computationally intensive offline phase and an online phase. In the offline phase, given access to an encryption oracle and choice of both the plaintexts and keys, the attacker generates a superpoly in terms of the key bits. This is evaluated on multiple chosen plaintexts in the online phase to get a linear system of polynomials. The name of the attack follows from the "cube" $y[I]$ in the superpoly, where $y[I]$ refers to a partial assignment of variables to a cartesian product $A_1 \times \cdots \times A_n$.

Several variants of cube attacks have been proposed, and were categorised in [COOP22]. While cube attacks mainly work on stream ciphers, a method of finding cube distinguishers for dynamic cube attacks on block ciphers was presented in [ARSA15] and the division property was used to find cube distinguishers in [EGB20].

OTHER ALGEBRAIC ATTACKS Other algebraic attacks include extended linearisation (XL), extended sparse linearisation (XSL) attack and Gröbner basis attack, including Buchberger's algorithm [Buc06], F4 [Fau99] and F5 [Fau02], and ElimLin [CB07].

These algorithms simplify and solve a system of equations with some constraints. Yang et al. give asymptotic security estimates under these attacks, by estimating the solving efficiency and observe that the attacks generally work better in conjunction with subkey guessing [YCC04]. In general, the complexity and efficiency of these algorithms are not agreed upon in the cryptographic community.

In the XSL attack introduced in [CP02], an attacker forms a system of multivariate quadratic (MQ) equations describing the cipher. Although MQ systems are generically hard to solve, in the AES and SERPENT cases, the systems are overdefined and sparse and thus solvable in slightly lower than brute force time complexity [CP02]. The attack uses a small number of plaintext-ciphertext pairs. Compared to other attacks like DC/LC, security against this attack does not grow exponentially with the number of rounds.

To counter this attack, Tran et al. studied SBox modifications to increase the algebraic complexity and reduce the sparsity of the MQ system [TBD08]. Meanwhile, Murphy—Robshaw considered a variant of the XSL attack on AES with all operations written in $GF(2^8)$ to simplify the system Mathematically [MR02]. However, the high degree of complexity in the attack makes it hard to estimate. The effectiveness of XSL attacks have been highly disputed [RM07, CL05].

Gröbner basis attacks have been applied to AES-256, with slightly better than brute force complexity [ZCX17]. Practically while there has been explicit construction of block ciphers that are resistant to DC/LC attacks but are weak against Gröbner basis attacks [BPW05], no cipher other than Keeloq has been proved vulnerable to algebraic attacks [CBW08].

MEET-IN-THE-MIDDLE AND VARIANTS The meet-in-the-middle attack was first introduced by Diffie–Hellman on Double DES [DH77]. The attack works by splitting the cipher into two components $E = E_1 \circ E_0$ as before. Given plaintext-ciphertext pairs, we may perform partial encryption (and respectively partial decryption), aiming to get a matching intermediate state.

If the round keys in E_1, E_0 are independent (as in the Double DES case), and assuming the case where E is split evenly, then partial encryption (and partial decryption) each only need to be done on half of the keyspace. This reduces the complexity from $2^{|K|}$ to $2^{|K|/2+1}$, however there is a memory tradeoff, as intermediate states have to be stored. For this attack to work, both E_1 and E_0 have to operate only using part of the key.

The meet-in-the-middle attack was extended by Demirci et al. to attack IDEA [DST03] and Demirci–Selçuk to attack AES [DS08a]. In these two papers, Meet-in-the-Middle is used as a generic framework to construct attacks from distinguishers. In their model, a cipher E is decomposed into three $E = E_2 \circ E_1 \circ E_0$, where there is a known distinguisher on the E_1, and only a portion of the key bits in E_0, E_2 are involved in the computation to test whether the distinguisher is satisfied. This approach, later known as Demirci-Selçuk meet-in-the-middle attack, has been applied to CLEFIA and camellia [LJWD15], as well as to generic balanced Feistel structures [GJNS14]. Improvements on the attack include Dunkelman et al.'s differential enumeration technique for memory data tradeoffs [DKS10].

To perform searches for Demirci-Selçuk meet-in-the-middle attacks, some automated tools have been developed including Derbez–Fouque's exhaustive search tool in C/C++ [DF16], Lin et al.'s integer optimization approach [LWWZ14] and Shi et al.'s constraint programming approach [SSD+18].

Another extension of Meet-in-the-Middle attacks are biclique attacks, which were first introduced against hash functions in [KRS12] and later extended to AES in [BKR11a], as well to PRESENT, Piccolo and LED [ÇKB12]. The main idea of biclique attacks is to partition the keyspace, so that one can use meet-in-the-middle attack. For each subset of keys S, one constructs a biclique, which is a complete bipartite graph where the edges match cipher round states values X to Y if there is a key from S such that X is encrypted to Y. The biclique is denoted as a set $\{\{X\}, \{Y\}, \{S\}\}$ of values from the key and two round states, and can be constructed from related key differentials [BKR11a]. In [AFL+14] Abed et al. developed a software framework to construct bicliques and determine the resulting attack complexity.

Other meet-in-the-middle attacks include collision attacks (including attacks in [WFC04]) and the slicing attack [Küh02], which we will not discuss in detail.

OTHER ATTACKS For attacks in this section, we only include the references to the first mentions, but leave further descriptions and methods of security evaluations of these attacks to future work.

Some attacks extend the cryptanalytic methods the sections above, exploring relations among a larger set of plaintext-ciphertext pairs. Examples of these include polytopic cryptanalysis [Tie16], which extends differential cryptanalysis (or impossible differential cryptanalysis), and partitioning cryptanalysis [HM97], which extends linear cryptanalysis. Other attacks combine several methods from the sections above, these include differential-bilinear attacks, higher-order linear attacks and combining boomerang with other attacks[BDK05a].

The related key approach has also been extended to make use of other distinguishers. The attacks under this framework include related key square, impossible differential, differential-linear and slide attacks. Generally, security evaluation again these other related key attacks are not specific to the attack model. Instead they are heuristic arguments that lack of uniformity in the key schedule suggests the ciphers' security against generic related key attacks, as in the security evaluation of SERPENT [ABK98].

Some other block cipher attacks we did not discuss above include the nonlinear invariant attack [TLS19], the invariant subspace attack [LAAZ11] (and a generalisation known as subspace trail attacks [GRR16]) and mixture differential cryptanalysis [Gra18] (also known as the exchange-invariant attack [BR19a]). We also did not cover attacks which investigate the general statistical features of ciphers, such as the bit distributions. These include the generic statistical attack, which was used on various ciphers including the following [GC90, GHJV00, Pes06].

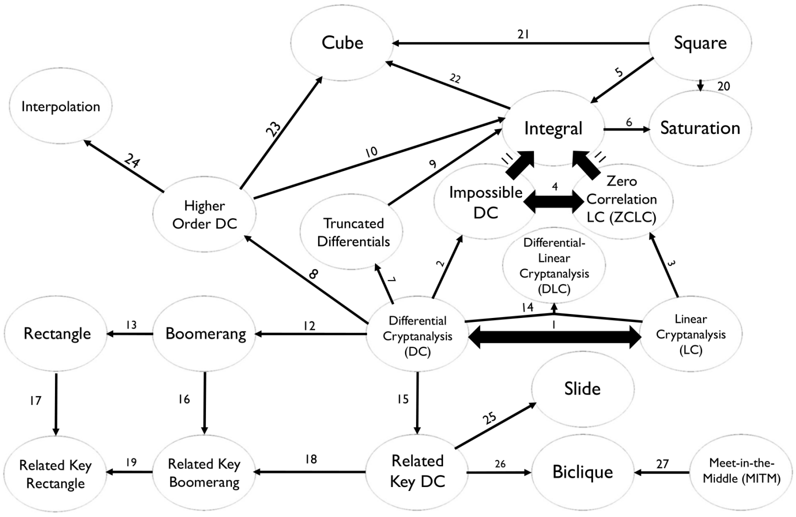


Figure 1: Map of how various attacks are related to each other. The edges indicate that the corresponding attacks are related. A more detailed explanation of these relations can be found in Section 4.1 and Table 3

4 Classifications and Connections

During the design process of a block cipher, it is paramount to consider the degree of effectiveness of various possible cryptanalytic techniques on the cipher. Due to the sheer volume of literature available on different attacks and their variants applied to different types of ciphers, the process of performing analysis of a new cipher design based on existing literature may be a highly daunting and involved task.

This section aims to ameliorate some of the pain during navigating the cipher design process by performing classifications on, and by drawing connections between, the different attacks presented in Section 3.

4.1 Association Map of Attacks

Here, we attempt to draw connections between different attacks through the use of an association map in Figure 1. This map presents these connections in a compact way for ease of reference, so that readers are able to observe the specific links between their attacks of interest at a glance. We note that the attacks and relations presented in this map are non-exhaustive. For instance, we omitted attacks such as the Slide Attack and Gröbner Basis Attacks as they do not connect well with the rest of the map. Additionally, we did not include the direct relation between Truncated Differentials and the Saturation Attack (i.e. that their distinguishers are identical up to a time-memory tradeoff [BN15]) as they are both connected through the Integral Attack, which we allude to in the map. For a more detailed exposition of these attacks and connections, we refer the reader to Section 3. Each node here corresponds to an attack and the edges between the nodes in the map indicates an association between the attacks in the nodes.

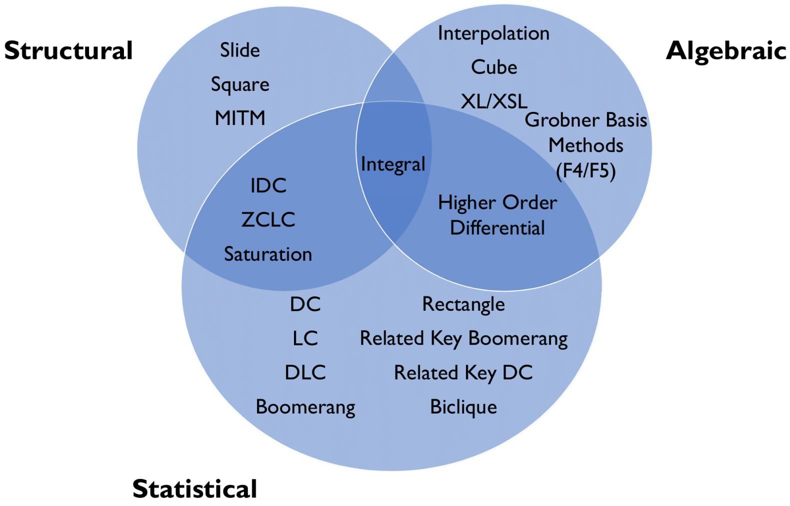


Figure 2: Rough classification of attacks based on approaches taken.

We hope that this map serves as a good starting reference for the study of block cipher cryptanalysis techniques. We shall provide a brief comment on the relations between the different attacks in Table 3 below. For the sake of brevity, we are unable to provide a complete discussion of the technical details of each relation in this paper. Instead, we refer the reader to the corresponding list of references in Table 3 to learn about the respective associations between the attacks in greater detail. Here, we opine that the DC, LC, Impossible DC, ZCLC and Integral attacks are the core attacks to consider during the block cipher evaluation process, in terms of their historical impact on existing ciphers and how influential or connected they are in relation to other attacks. For general purposes, we advise the reader to begin reading up on DC, and work through the map by traversing the edges in ascending order of their labels, and consulting their corresponding references in the table, as well as the references of any new attacks encountered in the process.

The thick arrows between the LC and DC nodes, as well as the IDC, ZCLC and Integral nodes, indicate extremely close and important associations between these attacks.

The connections between LC and DC are well known, and covered in Section 3 of this paper. In particular, the bi-directional edge between the LC and DC nodes refer to the one-to-one correspondence between the differential trails of a cipher structure $\mathcal{E}$ and linear hulls of its dual structure $\mathcal{E}^{\perp}$ [Mat95].

A ZC linear hull always indicates the presence of an integral distinguisher, while an $r-$round ID of a cipher structure $\mathcal{E}$ necessarily implies the existence of an $r-$round integral distinguisher of its dual structure $\mathcal{E}^{\perp}$. Additionally, there exists a one-to-one correspondence between IDs in a cipher structure $\mathcal{E}$ and ZC linear hulls in its dual structure $\mathcal{E}^{\perp}$ [SLR^{+}15]. Furthermore, it has been shown that once we have an ID distinguisher on r rounds involving M differentials, we obtain a ZC distinguisher on the same r rounds involving M linear approximations, and vice versa [BBW14].

Table 3: Descriptions of relations between attacks, and their corresponding references.

Edge Label	Description	Reference(s)
1	Mutually applicable on dual cipher structures, i.e. if there exists an $n-$round linear hull on cipher $\mathcal{E}$, then there exists an $n-$round differential trail on its dual structure $\mathcal{E}^{\perp}$.	[Bih95], [Mat95]
2	Probability Zero Characteristic.	[BBS99]
3	Correlation Zero Characteristic.	[BR11]
4	Mutually applicable on dual cipher structures, i.e. if there exists an $n-$round zero-correlation linear distinguisher on cipher $\mathcal{E}$, then there exists an $n-$round impossible differential trail on its dual structure $\mathcal{E}^{\perp}$.	[BLNW12]
5	Extension of Attack beyond AES-like ciphers.	[KW02]
6	Generalization to saturated subspaces which induce non-random output distributions.	[CS09]
7	Considering Multiple Sub-Differentials.	[Knu95]
8	Generalization to Higher Orders, i.e. taking derivatives $\Delta_{a_1,\ldots,a_i} f(x) = \Delta_{a_1,\ldots,a_{i-1}} f(x - a_i) - \Delta_{a_1,\ldots,a_{i-1}} f(x)$ for $i \geq 1$.	[Knu95]
9	Truncated Differential where the probability of having zero difference in q bits corresponds to the uniform probability $p = 2^q$, where q is the size of the output mask.	[KW02], [BN15]
10	Specific instance when considering $s-$order differentials over $\mathbb{F}_{2^k}$, where s is the size of the input mask. Related by the Division Property.	[KW02], [Tod15b]
11	Zero Correlation Linear Hull indicates the existence of an Integral Distinguisher. More specifically, an r-round Zero Correlation Linear Hull can be used to construct an r-round Integral Distinguisher. An Impossible Differential Distinguisher of cipher $\mathcal{E}$ always implies the existence of an Integral Distinguisher of its dual structure $\mathcal{E}^{\perp}$.	[BBW14], [SLR$^+$15]
12	Applied twice to two sub-ciphers.	[Wag99]
13	Targets differential characteristics over the entire space of intermediate differentials, rather than just the highest differential.	[BDK01]
14	DC applied to upper half of cipher, LC applied to lower half of cipher.	[LH94]
15	Applied to Key Schedule.	[Bih94], [KSW96]
16	Applied to Key Schedule.	[BDK05b]
17	Applied to Key Schedule.	[BDK05b]
18	Applied twice to two sub-ciphers.	[BDK05b]
19	Targets differential characteristics over the entire space of intermediate differentials, rather than just the highest differential.	[BDK05b]
20	Generalization to saturated subspaces which induce non-random output distributions.	[CS09]
21	Algebraic variant that also extracts secret variables from the characteristic.	[TIHM17]
22	Algebraic variant that also extracts secret variables from the characteristic.	[TIHM17]
23	Conceptually similar over $\mathbb{F}_2$.	[DS08b]
24	Generalization to recovering the coefficients of polynomials in s variables over $\mathbb{F}_{2^{m/s}}$, where m is the size of the PT/CT.	[JK01]
25	Variant of Related Key Attack, specifically when a cipher has self-related keys	[BDK08]
26	Often used in its construction.	[BKR11b]
27	Application with the aid of complete bipartite matchings, or bicliques, between intermediate states and key guesses.	[BKR11b]

4.2 Classification of Attacks

In Fig. 2, we classify the attacks into three categories: structural, statistical, and algebraic. The attacks belonging to each of these categories vary in their attack philosophy, in terms of their approach taken to derive distinguishers. This follows from generic literature on cryptanalytic techniques [Rim09, Jun05].

Structural attacks only require knowledge of the round structure of the cipher, without

Table 4: Adversarial models required for attacks. † DC may be a known PT attack under certain specific scenarios. ‡ Albeit rare, there exist known PT + chosen key difference RK differential attacks [Bih94]. ∗ There exists one instance of a CT-Only Slide Attack on DESX [BW00], and Slide Attacks may be improved under stronger adversarial models (Chosen PT/CT/ Adaptive Chosen PT etc.), provided the Weak Key Class exists.

Attack type	Attack Model
Differential	Chosen PT†
Linear	Known PT
Impossible Differential	Chosen PT
Zero Correlation LC	Known PT
Differential-Linear	Chosen PT
Boomerang	Adaptive Chosen PT/CT
Higher Order Differential	Chosen PT
RK Differential	Chosen PT‡ + Chosen Key Difference
RK Boomerang	Adaptive Chosen PT/CT + Chosen Key Difference
Integral	Chosen PT
Slide	Known PT∗ + Weak Key Class
Interpolation	Chosen PT + Possible Weak Key Class
MITM	Known PT/CT + Weak Key Schedule

details such as the specific functions or the SBox used. One of the earlier mentions of this branch of attack is in Structural Cryptanalysis of SASAS, where Biryukov and Shamir construct an attack which is independent of the specific SBox and affine functions in the encryption [BS01]. A textbook example of a structural attack is the integral attack.

Statistical attacks attempt to construct statistical patterns using plaintext ciphertext pairs, in order to distinguish the cipher from random permutations, using this to recover the key. These attacks exploit the probabilistic properties of block ciphers, and may require knowledge of the differential characteristics of SBoxes present in the ciphers.

Algebraic attacks exploit algebraic relations involving both the inputs and the outputs of some cipher component. The attacks often involve collecting, then solving a system of simultaneous equations in a large number of unknowns, possibly using algebraic tools.

Besides the above classification of attacks based on attack philosophy, we also observe that the security assumptions adopted by each attack is different. More specifically, some attacks have more stringent requirements than others that may render them impractical to a weaker adversarial model. These models may be classified into five broad categories, in descending order of strength: CT-Only, Known PT, Chosen PT, Chosen CT, and Adaptive Chosen PT/CT (i.e. it is easiest/ requires the least resources for an attacker to perform a CT-Only attack). In the following table, we shall summarize the (strongest) adversarial model enabled for a list of highlighted attacks.

5 Case Studies: Competition Schemes

In this case study, we are interested in how security evaluation has been done in popular SBox-based block ciphers *by the cryptography community.* This means we take into consideration not only the assurances and cryptanalysis performed by the scheme's designers, but also the subsequent work done in the literature to validate or invalidate these claims. Since many of the popular schemes used in real-world applications were proposed some time ago, there is a vast amount of associated security evaluation literature. As such, our case study serves two purposes: (1) as a survey of the cryptanalytic security evaluation of popular SBox-based block ciphers and (2) as a breadth-wise study comparing the claims made by scheme designers to subsequent results from the open literature. In short, we get a glimpse into how security evaluations of popular schemes mature over time.

In this section, we first overview how we delimited the case study. In Section 5.1, we provide a summary table (see Table 5) which covers the security claims made on nine popular schemes within the literature, and draw some conclusions from this. We also provide a detailed survey on the available literature for each of these schemes which were distilled to make Table 5 and cover some of the unique nuances that come with evaluating each scheme. However, in order to ensure comprehensiveness in these surveys we must defer it to Appendix 5.2 for brevity.

Scheme selection. Since we wanted our case study to encompass popular schemes that are used in real-world applications and have undergone substantial security analysis by academia, we looked to block cipher competitions which the international cryptography community participated actively in. Our schemes come from three sources:

- **Advanced Encryption Standard:** This NIST competition selected the block cipher AES (Rijndael) in 2001 [AES14]. We consider the five "finalists" of this competition in our case study.
- **CRYPTREC:** This was a process initiated by the Japanese government in 2000 to evaluate and recommend a broad set of cryptographic techniques for government and industry use [CRY22]. We consider all block ciphers from the "e-Government" and "Candidate" lists published in 2013.
- **NESSIE:** This was a European research project to identify secure cryptographic primitives that ran from 2000-2003. We consider all recommended block ciphers from this competition.

With the above shortlist, we omitted RC6 (from the AES process) and SHACAL-2 (from NESSIE) since they are not SBox-based block ciphers. We also omitted CIPHERUNICORN and 3-Key Triple DES (from CRYPTREC), since the former has not been studied extensively[1] and the latter will soon be deprecated for all applications by NIST [BR+18]. This left us with nine schemes: AES (Rijndael), Camellia, CLEFIA, Hierocrypt, MARS, MISTY1, SC2000, Serpent and Twofish.

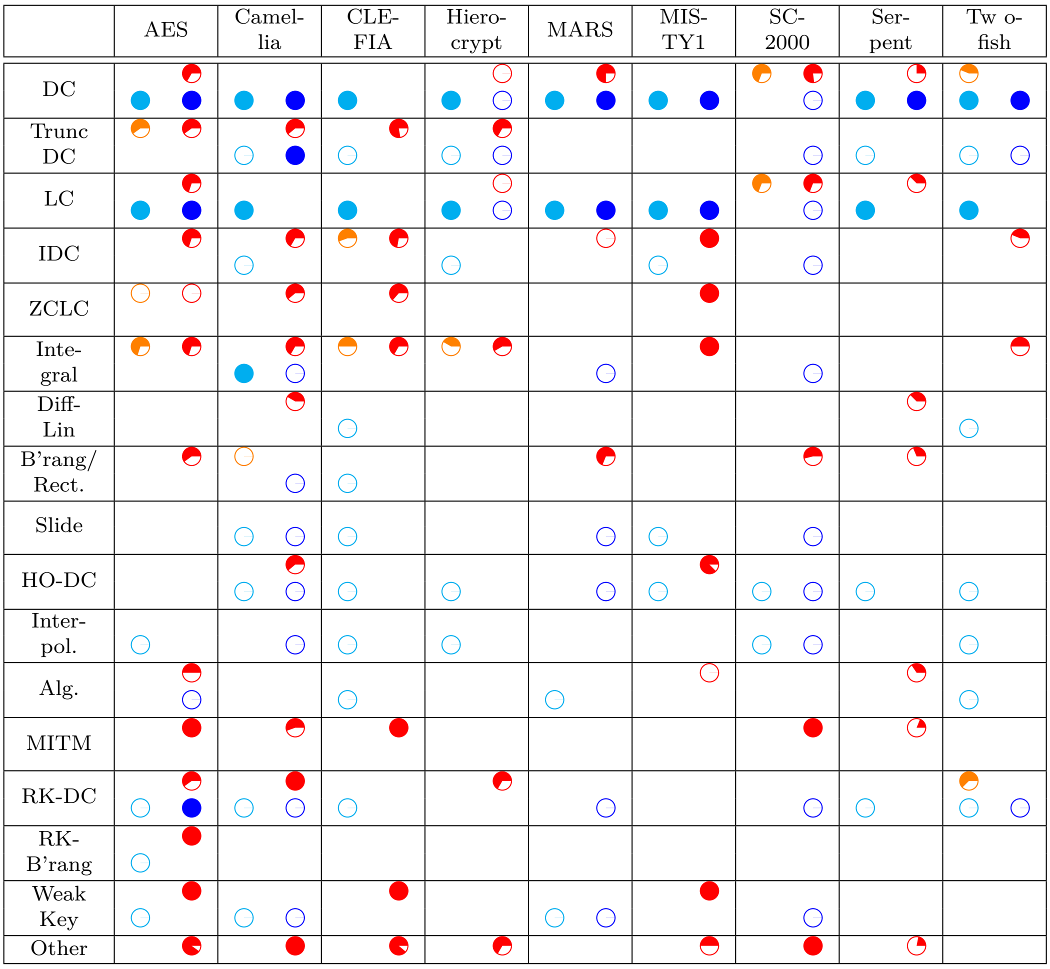
Survey Methodology. One can divide the claims made in cryptanalytic security evaluation literature into two groups which we call the "'defender POV" and "attacker POV". The intuitive difference is the stance taken by the authors – whether they are trying to prove that a scheme is secure or insecure. The "defender POV" includes any research done to provide assurances as to a scheme's resilience against particular forms of cryptanalysis. This includes more formal approaches, such as those discussed in Section 3, but also more heuristical arguments about why certain attacks would be "difficult to carry out", such as those that are used in design documents or subsequent security evaluations that are a part of the competition process. The "attacker POV" includes any work that attacks the scheme or a part thereof. This usually takes the form of cryptanalysis of round-reduced variants of the scheme, possibly with some scheme elements (e.g. whitening rounds) omitted.

In this case study, we included all works, to the best of our knowledge, which study the security of our schemes (or part thereof) in a standard attacker model in relation to one or more cryptanalytic techniques. In particular, we allow works that focus on reduced variants of the cipher (e.g. reduced round variants with no whitening rounds) but disallow further modifications to the scheme (e.g. variants with a secret SBox). In terms of the attacker model, we encompass all standard attacker models (e.g. chosen/known plaintexts, all-keys/weak-key attacks) but omit works which give the attacker additional inputs (e.g. side channel attacks). Also, for ease of comparison, this section will assume the adversary's goal is key-recovery (as opposed to distinguishing attacks) since that is the more potent model.

---

[1] Much of CIPHERUNICORN's documentation and evaluation was done in Japanese, so we were unable to include it.

Table 5: Summary of claims made in the security evaluation literature for nine popular SBox-based block ciphers from cryptographic competitions. In each cell, orange/ red dots indicate cryptanalysis work while cyan/blue dots indicate claims of security. In both cases, the color depends on whether the claims were made by the authors or in subsequent literature, respectively. Each dot's shading represents the gravity of the claim made (see Section 5.1 for details).



	AES	Camellia	CLEFIA	Hierocrypt	MARS	MISTY1	SC-2000	Serpent	Tw ofish
DC	◕ ● ●	● ●	●	○ ● ○	◕ ● ●	● ●	◕ ◕ ○	◔ ● ●	◔ ● ●
Trunc DC	◑ ◑	◑ ○ ●	◕ ○	◕ ○ ○			○	○	○ ○
LC	◕ ● ●	●	●	○ ● ○	● ●	● ●	◕ ◕ ○	◔ ●	●
IDC	◕	◕ ○	◑ ◕	○	○	● ○	○		◑
ZCLC	○ ○	◑	◑			●			
Integral	◕ ◕	◕ ● ○	◑ ◕	◔ ◑	○	●	○		◑
Diff-Lin		◔	○					◔	○
B'rang/ Rect.	◑	○ ○	○		◕		◑	◔	
Slide		○ ○	○		○	○	○		
HO-DC		◑ ○ ○	○	○	○	◕ ○	○ ○	○	○
Interpol.	○	○	○	○			○ ○		○
Alg.	◑ ○		○		○	○		◔	○
MITM	●	◑	●				●	◔	
RK-DC	◑ ○ ●	● ○ ○	○	◕	○		○	○	◑ ○ ○
RK-B'rang	● ○								
Weak Key	● ○	○ ○	●		○ ○	●	○		
Other	◕	●	◕	◕		◑	●	◔	

5.1 Breadthwise Study of Security Evaluations

In Table 5, we summarize the claims made for each scheme with respect to each of our cryptanalytic techniques. In each cell, we include up to four colored dots. Orange and red dots indicate cryptanalytic works by the authors and subsequent literature, respectively. The amount that the dot is colored in indicates the proportion of the full cipher that the most successful attack addresses. (e.g. ◔ would indicate that the cryptanalytic technique leads to a key-recovery attack on a variant of the cipher with a quarter of the rounds.) Note that an empty dot (i.e. ○ or ○) indicates that concerns have been raised about the scheme's security but no key-recovery attack has emerged (e.g. a distinguisher was found but not extended to a full attack). Cyan and blue indicate claims of security that have been made about the cipher. In particular, a filled dot (i.e. ● or ●) indicates a **proof of resistance** to the attack. This includes any formal analysis of why the cryptanalytic technique cannot be applied to the full cipher. On the other hand, an empty dot indicates a **claim of resistance** to the attack. This include all other claims that the scheme "should" resist the attack in question. This usually takes the form of heuristic arguments which explain why the attack would be "difficult to mount".

Since this is only intended as a broad overview for us to draw conclusions from, the table below simplifies the literature in a number of ways. First, in schemes with multiple key-sizes, the security claims apply to all variants and attacks reflected are the best performing one (in terms of the proportion of rounds) across all key sizes. Second, we include any attack that achieves a better time complexity than exhaustive search (i.e. they need not be "practical attacks"). Among works applying the same attack to the same scheme, we present only the maximal number of rounds for which a successful attack has been presented. Third, the rows associated to specific cryptanalytic techniques only consider attacks that work on the majority of keys. We gather all results that work on particular small classes of weak keys under the "Weak Key" row. Fourth, we acknowledge that works under the "defender POV" may present proofs in a variety of models, under very specific and different conditions. For example, some analyses are confined to certain special cases of the attacks or subclasses of differentials, or it may idealize portions of the scheme (e.g. SBoxes). For the sake of analysis, we generously permit all of these as "proofs" in the below table.

Due to the vast amount of literature covered by this table, we defer all citation details for Table 5 to after our analysis of the table. In Section 5.2 we provide some details on each scheme and links to their documentation. We also list all security claims and attacks that we are aware of for each scheme that were aggregated to form Table 5.

Discussion on Table 5. We acknowledge that there are many factors influencing how the research community as a whole handles the security evaluations of popular ciphers. However, we believe that there are still some interesting observations that can be drawn from Table 5. We now highlight some of these trends, and suggest some possible interpretations and avenues for future work that come out of them.

We observe that each cell where key-recovery attacks exist from both the authors and the subsequent literature, the latter always demonstrates improvement over the former. In Table 5, there is an average difference of 1.07 rounds, or 8.25% of the number of rounds in each full cipher. Additionally, we note that for each cryptanalytic attack from the literature presented in the table (i.e. the 54 non-empty dots in the top-right of cells) represents between 1 and 14 works, with an average of 3.69 works. These sequences of work steadily improved the rounds and complexities of the attack in question over the course of time. One takeaway that a scheme designer might draw from this is that *round-reduced cryptanalysis inevitably improves over time.* Therefore, if they use round-reduced cryptanalytic results of their own to justify their scheme's security against that form of cryptanalysis, they should incorporate a substantial number of buffering rounds to allow for cryptanalytic improvements over time. We believe that this buffer size is scheme-dependent, and may relate to the diffusion characteristics of the underlying round functions. This may constitute an interesting area for future work.

Now let's look at the relationship between the scheme's designers' security assurances (i.e. cyan dots) and cryptanalytic success (i.e. red dots). We note that the majority of the proofs (i.e. ●) concern the full cipher, so the presence of an attack does not invalidate the proof. For this analysis we only consider "significant" cryptanalytic efforts, which we define as breaking at least half of the rounds of the full cipher. From this, we can note that for all cells with assurances of security (i.e. ●/○), only 16 out of 55 (29.09%) have seen substantial attacks (i.e. red dot between ◓ and ●). This suggests a correlation between the cryptanalytic considerations during the design process and the security of the resultant cipher. This can be seen as evidence that *security evaluation via cryptanalytic techniques works.*

We also note that in the cases where an assurance of security (i.e. ●/○) was given but a full break was found (i.e. ●), it occurs when the assurance was done using heuristic techniques instead of a formal proof. We believe that this speaks to the *value of formal* *proof frameworks for deterring cryptanalysis* and believe that future work developing such would be well-received by cipher designers (much like Matsui's formalization of LC and DC [Mat95] which have been extended to the proof frameworks used by almost all our nine ciphers).

We can also draw some conclusions by looking at each scheme as its own case study. We note that one should be careful not to overgeneralize using Table 5. For example, AES having the "most red dots" is more likely to be a function of the popularity and visibility of this scheme, rather than an indicator that AES is the weakest cipher of the nine presented. However, our results provide at least anecdotal evidence that *discrepancies in security between comparable scheme may emerge over the course of time.* For example, SERPENT and MISTY1 were both proposed in 1998 with a very similar list of security assurances and comparable visibility (in terms of citations). However, since then, MISTY1 has been attacked much more successfully than SERPENT. While multiple cryptanalytic techniques have seen success when applied to full or almost-full-round MISTY1, SERPENT has not even seen an attack for more than 12 out of its 32 rounds. We see this as evidence that *scheme selection should not be rushed*, and that it may even be valuable to revisit the results of past selections and review cryptanalytic results that have emerged since then (similar to what CRYPTREC did in 2013 when they revisited their selected schemes and reorganized them into different tiers).

Reflections from Survey Process. At the close of this section, we make a couple final observations from the entire survey process that might be relevant to future work.

First, we feel that the study of block cipher cryptanalysis, especially from the POV of the attacker, is a very detailed-oriented and fiddly discipline. Great care must be taken to ensure the correctness, especially since most of the attacks exceed a practical amount of resources and cannot be verified via an implementation. Further evidence of this can be seen in the errors that have been pointed out in published cryptanalytic work which completely void the correctness of the attacks [Sch02, LK07, BNS14]. To address this, future work may consider formalizing adversarial models and a common syntax for classes of cryptanalytic attacks (perhaps extending our work in Section 3) to ease comparisons between different schemes, or even frameworks that simplify the verification of key-recovery attacks.

Second, it is worth noting that this area of research is both mature and vast. Our SoK covered a large portion of the literature out there, but we believe much more can be done to reorganize the area. In particular, future work may look to systemize cryptanalysis using side channels, alternate adversarial models, other block cipher types (e.g. ARX), or studying a wider breadth of schemes (e.g. authenticated encryption schemes from CAESAR [cae19]).

5.2 Summary of Cryptanalytic Results Against Competition Schemes.

Overview. Below we list works from the literature that we compiled to generate Table 5 in Section 5. For each of the nine schemes, we use two tables to capture the cryptanalytic works on that scheme and the security analyses of the scheme (respectively). We use the same color-coding as we did in Table 5 to differentiate between attacks/security claims and claims by the authors/subsequent work.

These works were all considered when constructing Table 5 with the exception of the algebraic XSL attacks (indicated with a † symbol) since the technique is controversial and has been questioned by many including [Sch02, LK07]. As discussed in Section 5, we consider an attack successful if it is able to break the cipher variant with lower time complexity than an exhaustive search. And for security claims, we distinguish between claims of security backed by rigorous mathematical proofs (i.e. which would likely indicate that applying the attack would be unproductive/impossible in a general sense) from those which indicate a likelihood of security (e.g. pointing out some design feature of the cipher which would likely resist the attack in question). Of course, this distinction at times requires us to make a subjective judgement call and future work could look into more nuanced ways to perform this classification.

Finally, as one might expect, not every piece of literature falls nicely into one of the cryptanalytic techniques we discussed. In our tables below, we try our best to faithfully represent techniques used. When compiling into Table 5, we gently relax some of the attack definitions to include closely related attack types, so that we can group as many attacks as we can under the list of major cryptanalytic techniques. We were able to group 154 out of 175 (88%) works in this way. Additionally, when cryptanalytic works present attacks on multiple similar cipher variants using the same cryptanalytic technique we only reflect the one which breaks the largest number of rounds.

AES (128-BIT RJINDAEL). Rjindael is an SPN cipher which won the NIST AES competition. AES was also selected among the recommended candidates in CRYPTREC and NESSIE. It has a 128-bit block, 128/192/256-bit keys, and 10/12/14 rounds, respectively.

In our study, we studied the cipher and claims given by the authors in the Rijndael specification document [AES01] and AES proposal [DR03], and compared them to those found in mainstream cryptography journals/conferences.

We summarize the works presenting key-recovery attacks on various reduced round variants of AES in Fig. 3. We also present security claims associated to AES in Fig. 4.

CAMELLIA. This is a GFN cipher that is recommended by CRYPTREC and NESSIE. Camellia has a 128-bit block, 128/192/256-bit keys, and 18/24/24 rounds, respectively.

In our study, we studied the cipher and claims given by the authors in their paper [AIK+01], the Camellia specification document [AIK+00] and supporting document [NC02], and compared them to those found in mainstream cryptography journals/conferences.

We summarize the works presenting key-recovery attacks on various variants of Camellia in Fig. 5. In addition to having reduced rounds, the works may also remove FL layers or whitening rounds from their variants. Since these significantly impact security, we indicate such variants in Fig. 5 as well. We also present security claims associated to Camellia in Fig. 6.

CLEFIA. CLEFIA is a GFN cipher recommended in CRYPTREC. CLEFIA has a 128-bit block, 128/192/256-bit keys, and 18/22/26 rounds, respectively.

In our study, we studied the cipher and claims given by the authors in their paper [SSA+07] and self-evaluation document[Son07], and compared them to those found in mainstream cryptography journals/conferences.

We summarize the works presenting key-recovery attacks on various variants of CLEFIA in Fig. 7. In addition to having reduced rounds, the works may also the whitening rounds from their variants. However, we believe that those attacks can be extended to include the key whitening rounds via the techniques used by [LJWD15]. We also present security claims associated to CLEFIA in Fig. 8.

HIEROCRYPT-L1. This is a recursively defined SPN cipher recommended in CRYPTREC. It has a 64-bit block and 128-bit keys. In the literature, this is sometimes described to have 6 rounds and other times as having 12 (SBox) layers. Below, we present all results in rounds for easy comparison. CRYPTREC also recommended the Hierocrypt-3 cipher, which has a very similar design but has a 128-bit block.

In our study, we studied the cipher and claims given by the authors in their paper [OMSK01], specification document [Cor01b] and self-evaluation document[Cor01a], and compared them to those found in mainstream cryptography journals/conferences.

We summarize the works presenting key-recovery attacks on various reduced round variants of Hierocrypt-L1 in Fig. 9. We also present security claims associated to Hierocrypt-L1 in Fig. 10.

Attack	# Rounds (by key len.)			Citation
	128-bit	192-bit	256-bit	
Trunc. DC	6	6	6	[AES01, DR03]
Integral	7	7	7	[AES01, DR03]
DC-MITM	4	4	4	[BDD+12]
DC		8	9	[Sas10]
Trunc. DC	6			[BGL19]
LC	7	7	7	[GM00]
IDC	5	5	5	[BK00]
IDC	6	6	6	[CKK+02]
IDC		7	7	[Pha04]
IDC	7			[BA07]
IDC	7	7	8	[ZWF07]
IDC	7	7	8	[LDKK08]
IDC	7			[MDRMH10]
IDC	7			[BLNS18]
IDC	7			[LP21]
Integral	6	6	6	[BK00]
Integral	6	7	7	[Tun12]
Integral	7	7	7	[L+00]
Integral	7	8	8	[FKL+01]
B'rang	6	6	6	[Bir04]
Alg. (Multiple-of-8)			7	[GRR17, BDK+18, BCC19]
Alg. (XSL)†	10	12	14	[CP02]
MITM		7	8	[DS08a]
MITM	7	7	8	[DTÇB09]
MITM	7	8	8	[DTÇB09]
MITM		8		[WLH10]
MITM		8	8	[DF14]
MITM	7	8	9	[DFJ13]
MITM		9	9	[LJW15]
MITM (Biclique)	10	12	14	[Bog12]
MITM (Biclique)	10	12	14	[BKR11a, GS13, BCGS15] [AFL+14, CNV13, TW15]
RK-DC	6			[SGL+17]
RK-DC		7	7	[ZWZF07]
RK-DC		8		[JD04]
RK-B'rang (Rect)		8		[HKLP05]
RK-B'rang		9		[GL08]
RK-B'rang (Rect)		9	10	[BDK05b, ZWZF07]
RK-B'rang (Rect)		10	10	[KHP07]
RK (Amp.) B'rang		12		[BK09]
RK-B'rang			14	[BK09]
RK-IDC	7	8	8	[ZWZF07]
RK-IDC		8	8	[BDK06]
RK-IDC		8	8	[ZWZF07]
RK-Integral	9	9	9	[FKL+01]
RK Diff-Lin		8		[ZZWF07]
Weak Key (RK-DC)	10	12	14	[BKN09]
Weak Key (RK B'rang)			10	[FGL09]
Rel. Subkey-DC			11	[BDK+10]
Diff. Enum.		8	8	[DKS10]
Imp. Polytopic	5	5	5	[Tie16]
Yoyo	5	5	5	[RBH17]
Mixture DC	6			[Gra17, BCC19, Gra19]

Figure 3: Key-Recovery attacks on reduced round variants of AES whose full variants contain 10/12/14 rounds respectively. These are the works on AES cryptanalysis that we surveyed to construct Fig. 5. (With the exception of controversial results labeled †.)

Attack	Security Claim	Citation
DC	●: Full AES is secure against DC attacks	[AES01, DR03]
LC	●: Full AES is secure against LC attacks	[AES01, DR03]
Interpol.	○: Diffusion layer provides security	[AES01, DR03]
Weak Key	○: IDEA weak key class	[AES01, DR03]
RK-Attacks	○: Key schedule offers security	[AES01, DR03]
DC	●: Full AES is secure against DC attacks	[PSC+02]
DC	○: Reduced round probability bound	[DR06]
LC	●: Full AES is secure against LC attacks	[PSC+02]
DC/LC	○: MILP analysis of ShiftRows' role in resisting DC/LC	[BJL+15]
IDC/ZCLC	○: No generic proof of without considering SBox details	[SLG+16]
Alg.	○: Resistance against known algebraic cryptanalysis	[Gho17]
Alg.	○: Simple algebraic presentations casts doubt on security	[FSW01, MR02] [BPW06]
RK-DC	●: Proof of active SBoxes in AES-128 in RK-setting	[KLPS17]
RK-DC	○: No generic proof of without considering MDS/SBox details. 9 round distinguisher has been found.	[FJP13]
Weak Key	○: Developed new framework which yields weak-key classes	[GLR+19]
Exchange	○: 6 round distinguisher has been found.	[BR19b, Bar19]

Figure 4: Security claims in the literature about AES' cryptanalysis. These are the AES analyses that we surveyed to construct Fig. 5.

MARS. This is a GFN cipher that was an AES finalist. It has a 128-bit block and 16 rounds, and allows the user to use between 128 to 448 key bits. However, since it was an AES finalist, it is often assumed to have 128, 192 or 256-bit keys.

In our study, we studied the cipher and claims given by the authors in their paper [BCD+99] and specification document [BCD+98], and compared them to those found in mainstream cryptography journals/conferences.

We summarize the works presenting key-recovery attacks on various reduced round variants of MARS in Fig. 11. We also present security claims associated to MARS in Fig. 12.

MISTY1. This is a GFN cipher that recommended by CRYPTREC and NESSIE. It has a 64-bit block, 128-bit key and a variable number of rounds (recommended: 8). KASUMI [rGPPG07], a popular cipher used in mobile telecommunications, is a variant of MISTY1.

In our study, we studied the cipher and claims given by the authors in their paper [Mat97] and supporting document [Mat00], and compared them to those found in mainstream cryptography journals/conferences.

We summarize the works presenting key-recovery attacks on various variants of MISTY1 in Fig. 13. In addition to having reduced rounds, the works may also remove some or all of the FL layers from their variants. In Fig. 13, the works indicated with a ✓ are those which consider any number of FL layers in their attacks, and those indicated with × considered none of them. We also present security claims associated to MISTY1 in Fig. 14.

SC2000. This is an SPN (by our definition) cipher recommended by CRYPTREC. It has a 128-bit block and 128/192/256-bit keys. SC2000 makes use of "I functions", "B functions" and "R functions", in a repeating IBIRR pattern with a trailing IBI for symmetry. In the original design, only the B and R functions were considered as "rounds", and the cipher was designed with 19/22/22 rounds (respectively). In subsequent literature, rounds are counted differently, with IBIRR being counted as a full round while IBI or RR are counted as half rounds. For consistency, we use the latter notation, meaning that SC2000 has 6.5/7.5/7.5 rounds (respectively).

In our study, we studied the cipher and claims given by the authors in their paper [SYY+02], and compared them to those found in mainstream cryptography journals/conferences.

Attack	# Rounds (by key len.)			FL	Whit-ening	Citation
	128-bit	192-bit	256-bit			
Trunc. DC	8			×	×	[LHL+02]
Trunc. DC	11	11	11	×	×	[SKI01]
Trunc. DC	11	12		✓	✓	[LJWD15]
IDC	12			×	×	[MSDB09]
IDC		10	11	✓	✓	[CJYW11]
IDC			15	×	×	[CJYW11]
IDC	11	12	14	✓	✓	[BL11]
IDC	10	11	12	✓	✓	[LCW11]
IDC		12	14	✓	×	[LCW11]
IDC	10	11	11	✓	✓	[LCJ11]
IDC		11	12	✓	✓	[LGL+11]
IDC	10	11	12	✓	✓	[LLG+12]
IDC	11	12		✓	✓	[LWFK12]
IDC		14	16	×	×	[LWFK12]
IDC		13	14	✓	×	[LGLL12]
IDC		13	14	✓	×	[Blo15]
IDC		14		✓	×	[JW16]
ZCLC		11	12	✓	×	[Bog12]
ZCLC	11	12		✓	✓	[BGW+14]
Integral	6			×	✓	[HQ01]
Integral			9	✓	×	[YPK02, LWFK12]
Integral	9		10	✓	✓	[LCF06]
Integral	9		11	×	×	[LCF06, LWFK12]
Integral	9		12	×	×	[LLF08, LWFK12]
Integral	10	12	12	×	×	[LWZZ11]
(MITM) Integral	10	11	12	✓	×	[LWKP12]
(MITM) Integral		14	16	×	×	[LWKP12]
Diff-Lin		9	10	×	×	[WF04]
HO-DC			11	×	×	[HSK03, LWFK12]
MITM			12	✓	✓	[CL12]
MITM	10	11	12	✓	×	[LWPF12]
MITM		12	13	✓	✓	[LJ14]
MITM	10	12	13	✓	✓	[DLJW15]
MITM (Biclique)	18	24	24	✓	✓	[Bog12]
RK-DC	18			×	×	[BN10]
Collision Searching	8	9	10	✓	✓	[WFC04]
Collision Searching	9	10	10	×	×	[WF03]

Figure 5: Key-Recovery attacks on reduced round variants of Camellia whose full variants contain 18/24/24 rounds respectively. These are the works on Camillia cryptanalysis that we surveyed to construct Fig. 5.

Attack	Security Claim	Citation
DC	●: Camellia is secure against DC attacks	[AIK+01, NC02]
Trunc. DC/LC	○: Found no attack on more than 10 rounds using [MT99, MSAK99] search methodology	[AIK+01, NC02]
LC	●: Camellia is secure against LC attacks	[AIK+01, NC02]
IDC	○: FL functions make IDC against full Camellia difficult	[AIK+01, NC02]
Integral/ interpol.	●: Searched for linear relations and proved no attack exists	[AIK+01, NC02]
B'rang	○: 8 round boomerang distinguisher found (no FL functions)	[AIK+01, NC02]
Slide	○: FL functions makes slide attack unlikely	[AIK+01, NC02]
HO-DC	○: High degree in SBox output makes HO-DC difficult	[AIK+01, NC02]
RK-DC	○: Key schedule makes RK-DC difficult	[AIK+01, NC02]
Weak Key	○: Key schedule makes equivalent key-classes unlikely	[AIK+01, NC02]
DC	●: No DC on more than 10 rounds	[BN12a]
DC/LC	○: No attacks on more than 10 rounds (no FL)	[SKA02]
Trunc. DC	●: No attacks on more than 11 rounds	[KM02]
Trunc. DC	●: No attacks on more than 7 rounds	[BN12a]
Integral	○: Integral less effective than trunc. DC	[CRY01a]
B'rang	○: "Approximately" 11 rounds will resist B'rang attack	[BN12a]
Slide/ Rotational	○: Structure not suited to these attacks	[BN12a]
HO-DC	○: High-degree SBox makes HO-DC difficult	[CRY01a]
Interpol.	○: Complex mathematical structure makes interpolation attack difficult	[CRY01a]
RK-DC	○: Structure makes these attack difficult	[CRY01a]
RK-DC	○: RK-DC (i.e. [BN10]) is infeasible	[BN12a]
Weak Key	○: Structure makes these attack difficult	[CRY01a]
Non-surjective	○: Structure makes these attack difficult	[CRY01a]
Mod n	○: Structure makes these attack difficult	[CRY01a]

Figure 6: Security claims in the literature about Camellia's cryptanalysis. These are the Camellia analyses that we surveyed to construct Fig. 5.

Attack	# Rounds (by key len.)			Whit-tening	Citation
	128-bit	192-bit	256-bit		
IDC	10	11	12	×	[SSA+07, Son07]
Integral	9	10	10	✓✗	[SSA+07, Son07]
Trunc. DC	14	14	15	×	[LJWD15]
IDC	12	13	14	✓	[WW07]
IDC	12	13	14	✓	[TTS+08b]
IDC	12	13	14	✓	[TTS+08a]
IDC	13			✓	[TSLL11]
IDC	13			✓	[MDS11]
IDC	13			✓	[BNS14]
ZCLC			13	✓	[BR11]
ZCLC		13	14	✓	[Bog12]
Multidim. ZCLC		14	15	✓	[BGW+14]
ZCLC		14	15	✓	[YC16]
Integral	12			✓	[SW13]
Integral	12	13	14	✓	[LWZ12]
Integral		14	15	✓	[YC16]
MITM (Biclique)	18	22	26	✓	[Bog12]
Weak Key (RK-DC)	18			✓	[ELN+14]
Imp. Diff-Lin	16			✓	[YLL13]
Improb. DC	13	14	15	✓	[Tez10]

Figure 7: Key-Recovery attacks on reduced round variants of CLEFIA whose full variants contain 18/22/26 rounds respectively. These are the works on CLEFIA cryptanalysis that we surveyed to construct Fig. 5.

Attack	Security Claim	Citation
DC	●: CLEFIA is secure against DC attacks	[SSA+07, Son07]
Trunc. DC	○: Distinguisher search suggests unlikely beyond 9 round on CLEFIA variant	[SSA+07, Son07]
LC	●: CLEFIA is secure against LC attacks	[SSA+07, Son07]
Trunc. LC	○: Implied by above DC result	[SSA+07, Son07]
Diff-Lin	○: Distinguisher search suggests this is worse than DC/LC. 8 round distinguisher has been found.	[SSA+07, Son07]
B'rang	○: Distinguisher search suggests unlikely beyond 9 rounds	[SSA+07, Son07]
Amp. B'rang	○: Distinguisher search suggests unlikely beyond 9 rounds	[SSA+07, Son07]
Rectangle	○: Estimates characteristic probability to be low, even though 10 round distinguisher is likely	[SSA+07, Son07]
Slide	○: Unlikely due to round constants	[SSA+07, Son07]
HO-DC	○: Unlikely due to high-degree SBoxes	[SSA+07, Son07]
Interpol.	○: Unlikely since number of terms needed to express SBoxes are high	[SSA+07, Son07]
Alg. (XSL)†	○: Estimates resources for XSL attack are impractical†	[SSA+07, Son07]
RK-DC	○: Probability estimates imply this is unlikely	[SSA+07, Son07]
Related cipher	○: Unlikely due to round constants	[SSA+07, Son07]
Collision	○: Suggests that collision techniques [GM00] may slightly improve integral attacks	[SSA+07, Son07]
χ^2	○: Unlikely since there are no useful correlations like those used against RC6 [Vau96, KM01]	[SSA+07, Son07]

Figure 8: Security claims in the literature about CLEFIA's cryptanalysis. These are the CLEFIA analyses that we surveyed to construct Fig. 5. (With the exception of controversial results labeled †.)

Attack	# Rounds	Citation
Integral	2.5	[OMSK01, Cor01a]
Trunc. DC	4	[ATY15]
Integral	3.5	[BRN+02]
RK-DC	4	[TMA14]
RK-IDC	4	[TMA14]

Figure 9: Key-Recovery attacks on reduced round variants of Hierocrypt-L1 whose full variant contains 6 rounds. These are the works on Hierocrypt-L1 cryptanalysis that we surveyed to construct Fig. 5.

Attack	Security Claim	Citation
DC	●: Full Hierocrypt-L1 is secure against DC attacks	[OMSK01, Cor01a]
Trunc. DC	○: Unlikely on more than 2.5 rounds	[OMSK01, Cor01a]
LC	●: Full Hierocrypt-L1 is secure against LC attacks	[OMSK01, Cor01a]
IDC	○: Hierocrypt design provides more resistance than AES	[OMSK01, Cor01a]
Integral	○: Hierocrypt design provides more resistance than AES	[OMSK01, Cor01a]
HO-DC	○: Unlikely due to high algebraic degree	[OMSK01, Cor01a]
Interpol.	○: Simple applications were ineffective	[OMSK01, Cor01a]
Non-Surjective	○: Unlikely due to cipher structure	[OMSK01, Cor01a]
Mod n	○: Unlikely due to cipher structure	[OMSK01, Cor01a]
χ^2	○: Unlikely due to cipher structure	[OMSK01, Cor01a]
DC	○: Provide upper bounds on security against DC	[OSSK01]
DC	○: Provide evidence that six rounds may not be enough	[Vau00a]
Trunc. DC	○: Unlikely due to cipher structure	[Vau00a]
LC	○: Provide upper bounds on security against DC	[OSSK01]
LC	○: Provide evidence that six rounds may not be enough	[Vau00a]

Figure 10: Security claims in the literature about Hierocrypt-L1's cryptanalysis. These are the Hierocrypt-L1 analyses that we surveyed to construct Fig. 5.

Attack	# Rounds (by key len.)			Citation
	128-bit	192-bit	256-bit	
DC			12	[GKL+11]
Amp. B'rang			11	[KKS01]

Figure 11: Key-Recovery attacks on reduced round variants of MARS whose full variants all contain 16 rounds. These are the works on MARS cryptanalysis that we surveyed to construct Fig. 5.

Attack	Security Claim	Citation
DC	●: MARS is secure against DC attacks	[BCD+99, BCD+98]
LC	●: MARS is secure against LC attacks	[BCD+99, BCD+98]
Alg.	○: Unlikely since it is not a group	[BCD+99, BCD+98]
Weak Key	○: Unlikely due to key expansion	[BCD+99, BCD+98]
Equiv. Keys	○: Unlikely due to key expansion	[BCD+99, BCD+98]
DC	●: MARS is secure against DC attacks	[CRY01b]
LC	●: MARS is secure against LC attacks	[CRY01b]
LC	○: Several works call into question the LC analysis [KR00, RY00, BCDM01], but no practical attack	[CRY01b]
IDC	○: 8 round distinguishers have been found	[BF00a]
Integral	○: Applies to MARS, but unlikely to exceed six rounds	[CRY01b]
Slide	○: Unlikely due to cipher structure	[CRY01b]
HO-DC	○: Unlikely due to high-degree SBox	[CRY01b]
RK-DC	○: Unlikely due to complex key schedule	[CRY01b]
Weak Key	○: Unlikely due to complex key schedule (MARS was changed to address weakness identified by [Saa99])	[CRY01b]
Non-Surjective	○: Unlikely due to cipher structure	[CRY01b]
Mod n	○: Unlikely due to cipher structure	[CRY01b]
Statistical	○: 8 rounds can be distinguished using "Book Stack" test	[Pes06]

Figure 12: Security claims in the literature about MARS' cryptanalysis. These are the MARS analyses that we surveyed to construct Fig. 5.

Attack	# Rounds	# FL	Citation
Slicing/ IDC	4	✓	[Küh02]
IDC	4	✓	[Küh01]
IDC	6	×	[Küh01]
IDC	6	✓	[LKKD08]
IDC/ Slicing	6	✓	[DK08]
IDC/ Slicing	7	×	[DK08]
IDC	7	✓	[JL12]
Multidim. ZCLC	7	✓	[YC14]
Integral	5	✓	[KW02]
Integral	6	✓	[SL09]
Integral	8	✓	[Tod15a]
Integral	8	✓	[Bar15a]
HO-DC	5	×	[THK99]
HO-DC	5	×	[BF01]
HO-DC	6	✓	[THSK08]
HO-DC	7	×	[THSK08]
HO-DC	7	✓	[TSSK09]
HO-DC	7	✓	[Bar15b]
Weak Key (RK-DC/ RK-B'rang)	8	✓	[LYW13]
Collision	4	✓	[Bih97, Küh01]

Figure 13: Key-Recovery attacks on reduced round variants of MISTY1 whose full variant is "recommended" to have 8 rounds. These are the works on MISTY1 cryptanalysis that we surveyed to construct Fig. 5.

Attack	Security Claim	Citation
DC	●: MISTY1 is secure against DC attacks	[Mat97, Mat00]
LC	●: MISTY1 is secure against LC attacks	[Mat97, Mat00]
IDC	○: Unlikely due to FL functions	[Mat97, Mat00]
Slide	○: Unlikely due to FL functions. (For variant with no FL, attack is slower than exhaustive.)	[Mat97, Mat00]
HO-DC	○: Unlikely due to algebraic structure and FL functions	[Mat97, Mat00]
DC	●: MISTY1 is secure against DC attacks	[LLSS10]
LC	●: MISTY1 is secure against LC attacks	[LLSS10]
IDC	○: Reduced round IDC likely, since multi round distinguishers exist	[LLSS10]
Integral	○: Reduced round Integral likely, since multi round distinguishers exist	[LLSS10]
HO-DC	○: SBox weakness enables the attacks by [THK99, BF01]	[CV02]
HO-DC	○: Reduced round distinguishers may yield HO-DC attacks	[Vau00b]
Alg.	○: Reduced round distinguishers may yield algebraic attacks	[Vau00b]
Weak Key	○: Subkey structure may yield weak keys	[Vau00b]
Generic Attacks	○: Minimum of 6 rounds required for security, even when assuming an idealized MISTY1	[NPT09, NPT10]

Figure 14: Security claims in the literature about MISTY1's cryptanalysis. These are the MISTY1 analyses that we surveyed to construct Fig. 5.

Attack	# Rounds (by key len.)			Citation
	128-bit	192-bit	256-bit	
DC	4.5	4.5	4.5	[SYY+02]
LC	4.5	4.5	4.5	[SYY+02]
DC	4.5	4.5	4.5	[RK01]
DC	4.5	4.5	4.5	[YSD02]
DC	5	5	5	[Lu10a]
LC	4.5	4.5	4.5	[YSD02]
B'rang	3.5	3.5	3.5	[BDK02c]
Rectangle	3.5	3.5	3.5	[BDK02c]
MITM (Biclique)	6.5	7.5	7.5	[Bog12]
Key Collision			7.5	[BN14, BN12b]

Figure 15: Key-Recovery attacks on reduced round variants of SC2000 whose full variants contain 6.5/7.5/7.5 rounds respectively. These are the works on SC2000 cryptanalysis that we surveyed to construct Fig. 5.

We summarize the works presenting key-recovery attacks on various reduced round variants of SC2000 in Fig. 15. We also present security claims associated to SC2000 in Fig. 16.

SERPENT. This is an SPN cipher that was an AES finalist. It has a 128-bit block, a key length of 256-bits (also 128 and 192 variants for the AES process), and 32 rounds.

In our study, we studied the cipher and claims given by the authors in their paper [BAK98] and specification document [ABK98], and compared them to those found in mainstream cryptography journals/conferences.

We summarize the works presenting key-recovery attacks on various reduced round variants of Serpent in Fig. 17. We also present security claims associated to Serpent in Fig. 18.

TWOFISH. This is an GFN cipher that was an AES finalist. It has a 128-bit block, any key length up to 256-bits (128/192/256 are the common lengths), and 16 rounds.

In our study, we studied the cipher and claims given by the authors in their specification document [SKW+98], and compared them to those found in mainstream cryptography journals/conferences.

We summarize the works presenting key-recovery attacks on various reduced round

Attack	Security Claim	Citation
HO-DC	○: Unlikely due to high degree polynomials	[SYY+02]
Interpol.	○: Unlikely due to variety and degree of algebraic structures	[SYY+02]
DC	○: Individual components seem to resist DC, but structure too complex to prove	[CRY01c]
Trunc. DC	○: Present evidence that Trunc. DC unlikely beyond 5 rounds	[CRY01c]
LC	○: Individual components seem to resist LC, but structure too complex to prove	[CRY01c]
IDC/RK-IDC	○: Unlikely due to high diffusion of word-based cipher	[BN12b]
Integral	○: Unlikely to do better than DC attacks	[CRY01c]
Slide	○: Unlikely due to key schedule	[CRY01c, BN12b]
HO-DC	○: Unlikely due to non-linearity of SBoxes	[CRY01c]
Interpol.	○: Unlikely due to design of SBoxes and B/R functions	[CRY01c]
RK-DC	○: Unlikely due to complex key schedule	[CRY01c]
Weak Key	○: Unlikely due to complex key schedule	[CRY01c]
Mod n	○: Unlikely to be applicable	[CRY01c]
Non-Surjective	○: Unlikely to be applicable	[CRY01c]
Rotational	○: Unlikely due to SBoxes and key schedule	[BN12b]

Figure 16: Security claims in the literature about SC2000's cryptanalysis. These are the SC2000 analyses that we surveyed to construct Fig. 5.

Attack	# Rounds (by key len.)			Citation
	128-bit	192-bit	256-bit	
DC	6	6	7	[KKS+00]
DC			8	[WW10]
Multi-DC	7	7	8	[WSTP12]
LC	10	11	11	[BDK02b]
LC	10	11	11	[CSQ07b]
LC	10	10	10	[Lu12, Lu10b]
LC/ Multi-LC	10	11	11	[CSQ07a, CSQ08]
Multi-LC	12	12	12	[NWW11]
Diff-Lin	10	11	11	[BDK03]
Diff-Lin	10	11	12	[DIK08]
Diff-Lin	10	11	12	[Lu12, Lu10b]
Diff-Lin	10	11	12	[TÖ14]
Diff-Lin			12	[BCD+21]
B'rang		8	8	[KKS+00]
Amp. B'rang		8	9	[KKS+00]
Amp. B'rang	8	8	8	[KKS01]
B'rang/Rect.	9	10	10	[BDK02c]
Rectangle	7	7	10	[BDK01]
Alg. (XSL)†	32	32	32	[CP02]
Alg. (Diff. Non-lin)			8	[WWH10]
Alg (Non-lin)	11	11	11	[MC13a, MC13b]
MITM			6	[KKS+00]
Improb. DC	7	7	7	[TTD14]

Figure 17: Key-Recovery attacks on reduced round variants of Serpent whose full variants all contain 32 rounds. These are the works on Serpect cryptanalysis that we surveyed to construct Fig. 5. (With the exception of controversial results labeled †.)

Attack	Security Claim	Citation
DC	●: Full Serpent is secure against DC attacks	[BAK98, ABK98]
Trunc. DC	○: Unlikely due to strong diffusion over many rounds	[BAK98, ABK98]
LC	●: Full Serpent is secure against LC attacks	[BAK98, ABK98]
HO-DC	○: Unlikely on more than 5 rounds, due to high-degree SBox	[BAK98, ABK98]
Alg. (Non-lin)	○: Unlikely to meaningfully improve upon LC due to large number of texts	[BAK98, ABK98]
RK-DC	○: Unlikely due to key schedule and multiple SBoxes	[BAK98, ABK98]
Statistical	○: Unlikely to be less complex than DC/LC	[BAK98, ABK98]
Partitioning	○: Unlikely to be less complex than DC/LC	[BAK98, ABK98]
DC	●: Serpent on 16 or more rounds is secure against DC	[WHC+00]
Multidim. LC	○: Multidimensional LC extends Multi-LC [CSQ07a, CSQ08]. 5 round distinguisher has been found.	[HCN08, CHN09]
Alg.	○: Non-linear order of SBox output bits misreported by authors, may yield algebraic attacks	[SAB09]

Figure 18: Security claims in the literature about Serpent's cryptanalysis. These are the Serpent analyses that we surveyed to construct Fig. 5.

Attack	# Rounds (by key len.)			Variant	Citation
	128-bit	192-bit	256-bit		
DC	5	5	5	×	[SKW+98]
DC	7	7	7	✓	[SKW+98]
RK-DC	10	10	10	✓	[SKW+98]
IDC	6	6	6	×	[Fer99]
IDC			6	✓	[Fer99]
IDC	7	7	7	×	[BF00b]
Integral	7	7	7	×	[Luc02]
Integral	8	8	8	✓	[Luc02]

Figure 19: Key-Recovery attacks on reduced round variants of Twofish whose full variants all contain 16 rounds. These are the works on Twofish cryptanalysis that we surveyed to construct Fig. 5.

variants of Twofish in Fig. 19. We also present security claims associated to Twofish in Fig. 20.

6 Conclusion

The block cipher design process is an intricate one, and it may be tricky to navigate the myriad of attacks and their conditions during security evaluation. In this paper, we presented a systemization of cryptanalysis of SBox-based block ciphers from a security evaluation standpoint. Additionally, we featured a unified common framework to present the attack techniques, generalizing distinguisher structures and consolidating respective formal and heuristic approaches to security evaluation. We also organized and compartmentalized the space of SBox-based block cipher attacks through graphical representations. Finally, we present a case study which draws conclusions about how security evaluation matures over time, with implications for future work.

References

[ABK98] Ross Anderson, Eli Biham, and Lars Knudsen. Serpent: A proposal for the advanced encryption standard. *NIST AES Proposal*, 174:1–23, 1998.

[AES01] Specification for the advanced encryption standard (aes). Federal Information Processing Standards Publication 197, 2001.

Attack	Security Claim	Citation
DC	●: Full Twofish is secure against DC attacks	[SKW+98]
Trunc. DC	○: Round function diffusion makes trunc. DC difficult	[SKW+98]
LC	●: Full Twofish is secure against LC attacks	[SKW+98]
Multiple LC	○: Unlikely since LC is unlikely	[SKW+98]
Generalized LC	○: Unlikely since statistical imbalances were not found	[SKW+98]
Diff-Lin	○: Unlikely due since DC component would cover most of cipher	[SKW+98]
HO-DC	○: No attacks on more than 6 rounds	[SKW+98]
Interpol.	○: Unlikely due to high algebraic degree of SBoxes	[SKW+98]
Alg. (Non-lin.)	○: Unlikely since LC is unlikely	[SKW+98]
RK-DC	○: Unlikely due to active SBoxes	[SKW+98]
RK-Slide	○: Attempted but unsuccessful	[SKW+98]
Partitioning	○: Attempted but unsuccessful	[SKW+98]
Partial Key	○: Unlikely due to strong key schedule	[SKW+98]
DC	●: 15 rounds will resist DC attack	[MR00]
Trunc. DC	○: Trunc. DC distinguishers [Knu00, MY00] does not necessarily extend to full attack	[Sch05]
RK-DC	○: Unlikely due to strong key schedule	[SKW+99]
RK-Slide	○: Unlikely due to strong key schedule	[SKW+99]
Equiv. Keys	○: Unlikely due to strong key schedule	[SKW+99]

Figure 20: Security claims in the literature about Twofish's cryptanalysis. These are the Twofish analyses that we surveyed to construct Fig. 5.

[AES14] Cryptographic competitions – aes: the advanced encryption standard. `https://competitions.cr.yp.to/aes.html`, 2014. Accessed: 2022-05-22.

[AFL+14] Farzaneh Abed, Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel. A framework for automated independent-biclique cryptanalysis. In Shiho Moriai, editor, *FSE 2013*, volume 8424 of *LNCS*, pages 561–581. Springer, Heidelberg, March 2014.

[AIK+00] Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita. Specification of camellia-a 128-bit block cipher. *Specification Version*, 2, 2000.

[AIK+01] Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita. Camellia: A 128-bit block cipher suitable for multiple platforms - Design and analysis. In Douglas R. Stinson and Stafford E. Tavares, editors, *SAC 2000*, volume 2012 of *LNCS*, pages 39–56. Springer, Heidelberg, August 2001.

[AKM97] Kazumaro Aoki, Kunio Kobayashi, and Shiho Moriai. Best differential characteristic search of FEAL. In Eli Biham, editor, *FSE'97*, volume 1267 of *LNCS*, pages 41–53. Springer, Heidelberg, January 1997.

[Aok00] Kazumaro Aoki. Efficient evaluation of security against generalized interpolation attack. In Howard Heys and Carlisle Adams, editors, *Selected Areas in Cryptography*, pages 135–146, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg.

[ARSA15] Zahra Ahmadian, Shahram Rasoolzadeh, Mahmoud Salmasizadeh, and Mohammad Reza Aref. Automated dynamic cube attack on block ciphers: Cryptanalysis of SIMON and KATAN. Cryptology ePrint Archive, Report 2015/040, 2015. `https://eprint.iacr.org/2015/040`.

[ATY15] Ahmed Abdelkhalek, Mohamed Tolba, and Amr M Youssef. Improved key recovery attack on round-reduced hierocrypt-l1 in the single-key setting. In

International Conference on Security, Privacy, and Applied Cryptography Engineering, pages 139–150. Springer, 2015.

[BA07] Behran Bahrak and Mohammad Reza Aref. A novel impossible differential cryptanalysis of aes. In *proceedings of the Western European Workshop on Research in Cryptology*, volume 2007. Citeseer, 2007.

[BAK98] Eli Biham, Ross J. Anderson, and Lars R. Knudsen. Serpent: A new block cipher proposal. In Serge Vaudenay, editor, *FSE'98*, volume 1372 of *LNCS*, pages 222–238. Springer, Heidelberg, March 1998.

[Bar15a] Achiya Bar-On. A 2^{70} attack on the full MISTY1. Cryptology ePrint Archive, Report 2015/746, 2015. https://eprint.iacr.org/2015/746.

[Bar15b] Achiya Bar-On. Improved higher-order differential attacks on MISTY1. In Gregor Leander, editor, *FSE 2015*, volume 9054 of *LNCS*, pages 28–47. Springer, Heidelberg, March 2015.

[Bar19] Navid Ghaedi Bardeh. A key-independent distinguisher for 6-round AES in an adaptive setting. Cryptology ePrint Archive, Report 2019/945, 2019. https://eprint.iacr.org/2019/945.

[BBD$^+$99] Eli Biham, Alex Biryukov, Orr Dunkelman, Eran Richardson, and Adi Shamir. Initial observations on Skipjack: Cryptanalysis of Skipjack-3XOR (invited talk). In Stafford E. Tavares and Henk Meijer, editors, *SAC 1998*, volume 1556 of *LNCS*, pages 362–376. Springer, Heidelberg, August 1999.

[BBS99] Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In Jacques Stern, editor, *EUROCRYPT'99*, volume 1592 of *LNCS*, pages 12–23. Springer, Heidelberg, May 1999.

[BBW14] Céline Blondeau, Andrey Bogdanov, and Meiqin Wang. On the (in)equivalence of impossible differential and zero-correlation distinguishers for Feistel- and Skipjack-type ciphers. In Ioana Boureanu, Philippe Owesarski, and Serge Vaudenay, editors, *ACNS 14*, volume 8479 of *LNCS*, pages 271–288. Springer, Heidelberg, June 2014.

[BCC19] Christina Boura, Anne Canteaut, and Daniel Coggia. A general proof framework for recent AES distinguishers. *IACR Trans. Symm. Cryptol.*, 2019(1):170–191, 2019.

[BCD$^+$98] Carolynn Burwick, Don Coppersmith, Edward D'Avignon, Rosario Gennaro, Shai Halevi, Charanjit Jutla, Stephen M Matyas Jr, Luke O'Connor, Mohammad Peyravian, David Safford, et al. Mars-a candidate cipher for aes. *NIST AES Proposal*, 268:80, 1998.

[BCD$^+$99] Carolynn Burwick, Don Coppersmith, Edward D'Avignon, Rosario Gennaro, Shai Halevi, Charanjit Jutla, Stephen M Matyas Jr, Luke O'Connor, Mohammad Peyravian, David Safford, et al. Mars-a candidate cipher for aes. *Citeseer*, 1999.

[BCD10] Christina Boura, Anne Canteaut, and Christophe De Cannière. Higher-order differential properties of Keccak and Luffa. Cryptology ePrint Archive, Report 2010/589, 2010. https://eprint.iacr.org/2010/589.

[BCD+21] Marek Broll, Federico Canale, Nicolas David, Antonio Florez-Gutierrez, Gregor Leander, María Naya-Plasencia, and Yosuke Todo. *Further improving differential-linear attacks: Applications to chaskey and serpent.* PhD thesis, IACR Cryptology ePrint Archive, 2021.

[BCDM01] L. Burnett, Gary Carter, Ed Dawson, and William Millan. Efficient methods for generating MARS-like S-boxes. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 300–314. Springer, Heidelberg, April 2001.

[BCGS15] Andrey Bogdanov, Donghoon Chang, Mohona Ghosh, and Somitra Kumar Sanadhya. Bicliques with minimal data and time complexity for AES. In Jooyoung Lee and Jongsung Kim, editors, *ICISC 14*, volume 8949 of *LNCS*, pages 160–174. Springer, Heidelberg, December 2015.

[BDD+12] Charles Bouillaguet, Patrick Derbez, Orr Dunkelman, Pierre-Alain Fouque, Nathan Keller, and Vincent Rijmen. Low-data complexity attacks on aes. *IEEE transactions on information theory*, 58(11):7002–7017, 2012.

[BDK01] Eli Biham, Orr Dunkelman, and Nathan Keller. The rectangle attack - rectangling the Serpent. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 340–357. Springer, Heidelberg, May 2001.

[BDK02a] Eli Biham, Orr Dunkelman, and Nathan Keller. Enhancing differential-linear cryptanalysis. In Yuliang Zheng, editor, *ASIACRYPT 2002*, volume 2501 of *LNCS*, pages 254–266. Springer, Heidelberg, December 2002.

[BDK02b] Eli Biham, Orr Dunkelman, and Nathan Keller. Linear cryptanalysis of reduced round Serpent. In Mitsuru Matsui, editor, *FSE 2001*, volume 2355 of *LNCS*, pages 16–27. Springer, Heidelberg, April 2002.

[BDK02c] Eli Biham, Orr Dunkelman, and Nathan Keller. New results on boomerang and rectangle attacks. In Joan Daemen and Vincent Rijmen, editors, *FSE 2002*, volume 2365 of *LNCS*, pages 1–16. Springer, Heidelberg, February 2002.

[BDK03] Eli Biham, Orr Dunkelman, and Nathan Keller. Differential-linear cryptanalysis of Serpent. In Thomas Johansson, editor, *FSE 2003*, volume 2887 of *LNCS*, pages 9–21. Springer, Heidelberg, February 2003.

[BDK05a] Eli Biham, Orr Dunkelman, and Nathan Keller. New combined attacks on block ciphers. In *International Workshop on Fast Software Encryption*, pages 126–144. Springer, 2005.

[BDK05b] Eli Biham, Orr Dunkelman, and Nathan Keller. Related-key boomerang and rectangle attacks. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 507–525. Springer, Heidelberg, May 2005.

[BDK06] Eli Biham, Orr Dunkelman, and Nathan Keller. Related-key impossible differential attacks on 8-round AES-192. In David Pointcheval, editor, *CT-RSA 2006*, volume 3860 of *LNCS*, pages 21–33. Springer, Heidelberg, February 2006.

[BDK07] Eli Biham, Orr Dunkelman, and Nathan Keller. Improved slide attacks. In Alex Biryukov, editor, *FSE 2007*, volume 4593 of *LNCS*, pages 153–166. Springer, Heidelberg, March 2007.

[BDK08] Eli Biham, Orr Dunkelman, and Nathan Keller. A unified approach to related-key attacks. In Kaisa Nyberg, editor, *FSE 2008*, volume 5086 of *LNCS*, pages 73–96. Springer, Heidelberg, February 2008.

[BDK+10] Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir. Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 299–319. Springer, Heidelberg, May / June 2010.

[BDK+18] Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir. Improved key recovery attacks on reduced-round AES with practical data and memory complexities. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 185–212. Springer, Heidelberg, August 2018.

[BF00a] Eli Biham and Vladimir Furman. Impossible differential on 8-round mars'core. In *AES Candidate Conference*, pages 186–194. Citeseer, 2000.

[BF00b] Eli Biham and Vladimir Furman. Improved impossible differentials on Twofish. In Bimal K. Roy and Eiji Okamoto, editors, *INDOCRYPT 2000*, volume 1977 of *LNCS*, pages 80–92. Springer, Heidelberg, December 2000.

[BF01] Steve Babbage and Laurent Frisch. On MISTY1 higher order differential cryptanalysis. In Dongho Won, editor, *ICISC 00*, volume 2015 of *LNCS*, pages 22–36. Springer, Heidelberg, December 2001.

[BGL19] Zhenzhen Bao, Jian Guo, and Eik List. Extended expectation cryptanalysis on round-reduced AES. Cryptology ePrint Archive, Report 2019/622, 2019. https://eprint.iacr.org/2019/622.

[BGW+14] Andrey Bogdanov, Huizheng Geng, Meiqin Wang, Long Wen, and Baudoin Collard. Zero-correlation linear cryptanalysis with FFT and improved attacks on ISO standards Camellia and CLEFIA. In Tanja Lange, Kristin Lauter, and Petr Lisonek, editors, *SAC 2013*, volume 8282 of *LNCS*, pages 306–323. Springer, Heidelberg, August 2014.

[BHL+20] Hamid Boukerrou, Paul Huynh, Virginie Lallemand, Bimal Mandal, and Marine Minier. On the Feistel counterpart of the boomerang connectivity table (long paper). *IACR Trans. Symm. Cryptol.*, 2020(1):331–362, 2020.

[Bih94] Eli Biham. New types of cryptanalytic attacks using related keys (extended abstract). In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *LNCS*, pages 398–409. Springer, Heidelberg, May 1994.

[Bih95] Eli Biham. On Matsui's linear cryptanalysis. In Alfredo De Santis, editor, *EUROCRYPT'94*, volume 950 of *LNCS*, pages 341–355. Springer, Heidelberg, May 1995.

[Bih97] Eli Biham. Cryptanalysis of Ladder-DES. In Eli Biham, editor, *FSE'97*, volume 1267 of *LNCS*, pages 134–138. Springer, Heidelberg, January 1997.

[Bir04] Alex Biryukov. The boomerang attack on 5 and 6-round reduced aes. In *International Conference on Advanced Encryption Standard*, pages 11–15. Springer, 2004.

[BJL$^+$15] Christof Beierle, Philipp Jovanovic, Martin M. Lauridsen, Gregor Leander, and Christian Rechberger. Analyzing permutations for AES-like ciphers: Understanding ShiftRows. In Kaisa Nyberg, editor, *CT-RSA 2015*, volume 9048 of *LNCS*, pages 37–58. Springer, Heidelberg, April 2015.

[BK00] Eli Biham and Nathan Keller. Cryptanalysis of reduced variants of rijndael. In *3rd AES Conference*, volume 230, 2000.

[BK09] Alex Biryukov and Dmitry Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 1–18. Springer, Heidelberg, December 2009.

[BKN09] Alex Biryukov, Dmitry Khovratovich, and Ivica Nikolic. Distinguisher and related-key attack on the full AES-256. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 231–249. Springer, Heidelberg, August 2009.

[BKR11a] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique cryptanalysis of the full AES. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 344–371. Springer, Heidelberg, December 2011.

[BKR11b] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique cryptanalysis of the full AES. Cryptology ePrint Archive, Report 2011/449, 2011. https://eprint.iacr.org/2011/449.

[BL11] Dongxia Bai and Leibo Li. New impossible differential attacks on Camellia. Cryptology ePrint Archive, Report 2011/661, 2011. https://eprint.iacr.org/2011/661.

[BLN15] Céline Blondeau, Gregor Leander, and Kaisa Nyberg. Differential-linear cryptanalysis revisited. In Carlos Cid and Christian Rechberger, editors, *FSE 2014*, volume 8540 of *LNCS*, pages 411–430. Springer, Heidelberg, March 2015.

[BLNS18] Christina Boura, Virginie Lallemand, María Naya-Plasencia, and Valentin Suder. Making the impossible possible. *Journal of Cryptology*, 31(1):101–133, January 2018.

[BLNW12] Andrey Bogdanov, Gregor Leander, Kaisa Nyberg, and Meiqin Wang. Integral and multidimensional linear distinguishers with correlation zero. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 244–261. Springer, Heidelberg, December 2012.

[Blo15] Céline Blondeau. Impossible differential attack on 13-round camellia-192. *Information Processing Letters*, 115(9):660–666, 2015.

[BN10] Alex Biryukov and Ivica Nikolic. Automatic search for related-key differential characteristics in byte-oriented block ciphers: Application to AES, Camellia, Khazad and others. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 322–344. Springer, Heidelberg, May / June 2010.

[BN12a] Alex Biryukov and Ivica Nikolić. Security analysis of the block cipher camellia. https://www.cryptrec.go.jp/exreport/cryptrec-ex-2202-2012p1.pdf, 2012. Accessed: 2022-05-22.

[BN12b] Alex Biryukov and Ivica Nikolić. Security analysis of the block cipher sc2000. https://www.cryptrec.go.jp/exreport/cryptrec-ex-2202-2012p3.pdf, 2012. Accessed: 2022-05-22.

[BN14] Alex Biryukov and Ivica Nikolic. Colliding keys for SC2000-256. In Antoine Joux and Amr M. Youssef, editors, *SAC 2014*, volume 8781 of *LNCS*, pages 77–91. Springer, Heidelberg, August 2014.

[BN15] Céline Blondeau and Kaisa Nyberg. On distinct known plaintext attacks. In *WCC2015-9th International Workshop on Coding and Cryptography 2015*, 2015.

[BNS14] Christina Boura, María Naya-Plasencia, and Valentin Suder. Scrutinizing and improving impossible differential attacks: Applications to CLEFIA, Camellia, LBlock and Simon (full version). Cryptology ePrint Archive, Report 2014/699, 2014. `https://eprint.iacr.org/2014/699`.

[Bog12] Andrey Bogdanov. Security evaluation of block ciphers aes, camellia,clefia and sc2000 using two new techniques: Biclique attacks and zero-correlation linear attacks. `https://www.cryptrec.go.jp/exreport/cryptrec-ex-2204-2012.pdf`, 2012. Accessed: 2022-05-22.

[BPW05] Johannes Buchmann, Andrei Pychkine, and Ralf-Philipp Weinmann. Block ciphers sensitive to Groebner basis attacks. Cryptology ePrint Archive, Report 2005/200, 2005. `https://eprint.iacr.org/2005/200`.

[BPW06] Johannes Buchmann, Andrei Pyshkin, and Ralf-Philipp Weinmann. A zero-dimensional Gröbner basis for AES-128. In Matthew J. B. Robshaw, editor, *FSE 2006*, volume 4047 of *LNCS*, pages 78–88. Springer, Heidelberg, March 2006.

[BR11] Andrey Bogdanov and Vincent Rijmen. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. Cryptology ePrint Archive, Report 2011/123, 2011. `https://eprint.iacr.org/2011/123`.

[BR$^+$18] Elaine Barker, Allen Roginsky, et al. Revision 2: Transitioning the use of cryptographic algorithms and key lengths. *NIST Special Publication*, 800:131A, 2018.

[BR19a] Navid Ghaedi Bardeh and Sondre Rønjom. The exchange attack: How to distinguish six rounds of AES with $2^{88.2}$ chosen plaintexts. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 347–370. Springer, Heidelberg, December 2019.

[BR19b] Navid Ghaedi Bardeh and Sondre Rønjom. The exchange attack: How to distinguish six rounds of AES with $2^{88.2}$ chosen plaintexts. Cryptology ePrint Archive, Report 2019/652, 2019. `https://eprint.iacr.org/2019/652`.

[BRN$^+$02] Paulo S. L. M. Barreto, Vincent Rijmen, Jorge Nakahara Jr., Bart Preneel, Joos Vandewalle, and Hae Yong Kim. Improved SQUARE attacks against reduced-round HIEROCRYPT. In Mitsuru Matsui, editor, *FSE 2001*, volume 2355 of *LNCS*, pages 165–173. Springer, Heidelberg, April 2002.

[BS91] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, January 1991.

[BS01] Alex Biryukov and Adi Shamir. Structural cryptanalysis of SASAS. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 394–405. Springer, Heidelberg, May 2001.

[Buc06] Bruno Buchberger. Bruno buchberger's phd thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of symbolic computation*, 41(3-4):475–511, 2006.

[BW99] Alex Biryukov and David Wagner. Slide attacks. In Lars R. Knudsen, editor, *FSE'99*, volume 1636 of *LNCS*, pages 245–259. Springer, Heidelberg, March 1999.

[BW00] Alex Biryukov and David Wagner. Advanced slide attacks. In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 589–606. Springer, Heidelberg, May 2000.

[BW12] Andrey Bogdanov and Meiqin Wang. Zero correlation linear cryptanalysis with reduced data complexity. In Anne Canteaut, editor, *FSE 2012*, volume 7549 of *LNCS*, pages 29–48. Springer, Heidelberg, March 2012.

[BZL15] Zhenzhen Bao, Wentao Zhang, and Dongdai Lin. Speeding up the search algorithm for the best differential and best linear trails. In Dongdai Lin, Moti Yung, and Jianying Zhou, editors, *Information Security and Cryptology*, pages 259–285, Cham, 2015. Springer International Publishing.

[cae19] Cryptographic competitions – caesar: Competition for authenticated encryption: Security, applicability, and robustness. `https://competitions.cr.yp.to/caesar.html`, 2019. Accessed: 2022-05-22.

[CB07] Nicolas Courtois and Gregory V. Bard. Algebraic cryptanalysis of the data encryption standard. In Steven D. Galbraith, editor, *11th IMA International Conference on Cryptography and Coding*, volume 4887 of *LNCS*, pages 152–169. Springer, Heidelberg, December 2007.

[CBW08] Nicolas Courtois, Gregory V. Bard, and David Wagner. Algebraic and slide attacks on KeeLoq. In Kaisa Nyberg, editor, *FSE 2008*, volume 5086 of *LNCS*, pages 97–115. Springer, Heidelberg, February 2008.

[CHN09] Joo Yeon Cho, Miia Hermelin, and Kaisa Nyberg. A new technique for multidimensional linear cryptanalysis with applications on reduced round Serpent. In Pil Joong Lee and Jung Hee Cheon, editors, *ICISC 08*, volume 5461 of *LNCS*, pages 383–398. Springer, Heidelberg, December 2009.

[CHP$^+$18] Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. Boomerang connectivity table: A new cryptanalysis tool. Cryptology ePrint Archive, Report 2018/161, 2018. `https://eprint.iacr.org/2018/161`.

[CJF$^+$16] Tingting Cui, Keting Jia, Kai Fu, Shiyao Chen, and Meiqin Wang. New automatic search tool for impossible differentials and zero-correlation linear approximations. Cryptology ePrint Archive, Report 2016/689, 2016. `https://eprint.iacr.org/2016/689`.

[CJYW11] Jiazhe Chen, Keting Jia, Hongbo Yu, and Xiaoyun Wang. New impossible differential attacks of reduced-round Camellia-192 and Camellia-256. In Udaya Parampalli and Philip Hawkes, editors, *ACISP 11*, volume 6812 of *LNCS*, pages 16–33. Springer, Heidelberg, July 2011.

[ÇKB12] Mustafa Çoban, Ferhat Karakoç, and Özkan Boztaş. Biclique cryptanalysis of TWINE. Cryptology ePrint Archive, Report 2012/422, 2012. `https://eprint.iacr.org/2012/422`.

[CKK$^+$02] Jung Hee Cheon, MunJu Kim, Kwangjo Kim, Jung-Yeun Lee, and SungWoo Kang. Improved impossible differential cryptanalysis of Rijndael and Crypton. In Kwangjo Kim, editor, *ICISC 01*, volume 2288 of *LNCS*, pages 39–49. Springer, Heidelberg, December 2002.

[CL05] Carlos Cid and Gaëtan Leurent. An analysis of the XSL algorithm. In Bimal K. Roy, editor, *ASIACRYPT 2005*, volume 3788 of *LNCS*, pages 333–352. Springer, Heidelberg, December 2005.

[CL12] Jiazhe Chen and Leibo Li. Low data complexity attack on reduced Camellia-256. In Willy Susilo, Yi Mu, and Jennifer Seberry, editors, *ACISP 12*, volume 7372 of *LNCS*, pages 101–114. Springer, Heidelberg, July 2012.

[CNV13] Anne Canteaut, María Naya-Plasencia, and Bastien Vayssière. Sieve-in-the-middle: Improved MITM attacks. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 222–240. Springer, Heidelberg, August 2013.

[COOP22] Marco Cianfriglia, Elia Onofri, Silvia Onofri, and Marco Pedicini. Ten years of cube attacks. *Cryptology ePrint Archive*, 2022.

[Cor01a] Toshiba Corporation. Self evaluation : Hierocrypt—l1. `https://www.global.toshiba/content/dam/toshiba/ww/technology/corporate/rdc/security/hcl1_01eeval.pdf`, 2001. Accessed: 2022-05-22.

[Cor01b] Toshiba Corporation. Specification on a block cipher : Hierocrypt—l1. `https://www.cryptrec.go.jp/en/cryptrec_03_spec_cypherlist_files/PDF/04_02espec.pdf`, 2001. Accessed: 2022-05-22.

[CP02] Nicolas Courtois and Josef Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In Yuliang Zheng, editor, *ASIACRYPT 2002*, volume 2501 of *LNCS*, pages 267–287. Springer, Heidelberg, December 2002.

[CRY01a] CRYPTREC. Analysis of camellia. `https://www.cryptrec.go.jp/exreport/cryptrec-ex-1082-2000.pdf`, 2001. Accessed: 2022-05-22.

[CRY01b] CRYPTREC. Analysis of mars. `https://www.cryptrec.go.jp/exreport/cryptrec-ex-1085-2000.pdf`, 2001. Accessed: 2022-05-22.

[CRY01c] CRYPTREC. Analysis of sc2000. `https://www.cryptrec.go.jp/exreport/cryptrec-ex-1087-2000.pdf`, 2001. Accessed: 2022-05-22.

[CRY22] Cryptrec: Cryptography research and evaluation committees. `https://www.cryptrec.go.jp/`, 2022. Accessed: 2022-05-22.

[CS09] Baudoin Collard and François-Xavier Standaert. A statistical saturation attack against the block cipher PRESENT. In Marc Fischlin, editor, *CT-RSA 2009*, volume 5473 of *LNCS*, pages 195–210. Springer, Heidelberg, April 2009.

[CSQ07a] Baudoin Collard, F-X Standaert, and J-J Quisquater. Improved and multiple linear cryptanalysis of reduced round serpent. In *International Conference on Information Security and Cryptology*, pages 51–65. Springer, 2007.

[CSQ07b] Baudoin Collard, François-Xavier Standaert, and Jean-Jacques Quisquater. Improving the time complexity of Matsui's linear cryptanalysis. In Kil-Hyun Nam and Gwangsoo Rhee, editors, *ICISC 07*, volume 4817 of *LNCS*, pages 77–88. Springer, Heidelberg, November 2007.

[CSQ08] Baudoin Collard, François-Xavier Standaert, and Jean-Jacques Quisquater. Experiments on the multiple linear cryptanalysis of reduced round Serpent. In Kaisa Nyberg, editor, *FSE 2008*, volume 5086 of *LNCS*, pages 382–397. Springer, Heidelberg, February 2008.

[CV02] Anne Canteaut and Marion Videau. Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis. In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 518–533. Springer, Heidelberg, April / May 2002.

[CZK⁺11] Jiali Choy, Aileen Zhang, Khoongming Khoo, Matt Henricksen, and Axel Poschmann. AES variants secure against related-key differential and boomerang attacks. Cryptology ePrint Archive, Report 2011/072, 2011. https://eprint.iacr.org/2011/072.

[Dae95] Joan Daemen. *Cipher and hash function design strategies based on linear and differential cryptanalysis*. PhD thesis, Doctoral Dissertation, March 1995, KU Leuven, 1995.

[DDK09] Christophe De Cannière, Orr Dunkelman, and Miroslav Knežević. KATAN and KTANTAN - a family of small and efficient hardware-oriented block ciphers. In Christophe Clavier and Kris Gaj, editors, *CHES 2009*, volume 5747 of *LNCS*, pages 272–288. Springer, Heidelberg, September 2009.

[DDKS15] Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Reflections on slide with a twist attacks. *Designs, Codes and Cryptography*, 77(2):633–651, 2015.

[DDV20] Stéphanie Delaune, Patrick Derbez, and Mathieu Vavrille. Catching the fastest boomerangs application to SKINNY. *IACR Trans. Symm. Cryptol.*, 2020(4):104–129, 2020.

[DF14] Patrick Derbez and Pierre-Alain Fouque. Exhausting Demirci-Selçuk meet-in-the-middle attacks against reduced-round AES. In Shiho Moriai, editor, *FSE 2013*, volume 8424 of *LNCS*, pages 541–560. Springer, Heidelberg, March 2014.

[DF16] Patrick Derbez and Pierre-Alain Fouque. Automatic search of meet-in-the-middle and impossible differential attacks. Cryptology ePrint Archive, Report 2016/579, 2016. https://eprint.iacr.org/2016/579.

[DFJ13] Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean. Improved key recovery attacks on reduced-round AES in the single-key setting. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 371–387. Springer, Heidelberg, May 2013.

[DH77] Whitfield Diffie and Martin E. Hellman. Special feature exhaustive cryptanalysis of the nbs data encryption standard. *Computer*, 10:74–84, 1977.

[DIK08] Orr Dunkelman, Sebastiaan Indesteege, and Nathan Keller. A differential-linear attack on 12-round Serpent. In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, *INDOCRYPT 2008*, volume 5365 of *LNCS*, pages 308–321. Springer, Heidelberg, December 2008.

[DK08] Orr Dunkelman and Nathan Keller. An improved impossible differential attack on MISTY1. In Josef Pieprzyk, editor, *ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 441–454. Springer, Heidelberg, December 2008.

[DKR97] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The block cipher SQUARE. In Eli Biham, editor, *FSE'97*, volume 1267 of *LNCS*, pages 149–165. Springer, Heidelberg, January 1997.

[DKS10] Orr Dunkelman, Nathan Keller, and Adi Shamir. Improved single-key attacks on 8-round AES-192 and AES-256. In Masayuki Abe, editor, *ASIACRYPT 2010*, volume 6477 of *LNCS*, pages 158–176. Springer, Heidelberg, December 2010.

[DKS14] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. *Journal of Cryptology*, 27(4):824–849, October 2014.

[DLJW15] Xiaoyang Dong, Leibo Li, Keting Jia, and Xiaoyun Wang. Improved attacks on reduced-round Camellia-128/192/256. In Kaisa Nyberg, editor, *CT-RSA 2015*, volume 9048 of *LNCS*, pages 59–83. Springer, Heidelberg, April 2015.

[DLMW15] Itai Dinur, Yunwen Liu, Willi Meier, and Qingju Wang. Optimized interpolation attacks on LowMC. Cryptology ePrint Archive, Report 2015/418, 2015. https://eprint.iacr.org/2015/418.

[DR01] Joan Daemen and Vincent Rijmen. The wide trail design strategy. In Bahram Honary, editor, *8th IMA International Conference on Cryptography and Coding*, volume 2260 of *LNCS*, pages 222–238. Springer, Heidelberg, December 2001.

[DR03] Joan Daemen and Vincent Rijmen. Aes proposal: Rijndael. NIST, 2003.

[DR06] Joan Daemen and Vincent Rijmen. Understanding two-round differentials in AES. In Roberto De Prisco and Moti Yung, editors, *SCN 06*, volume 4116 of *LNCS*, pages 78–94. Springer, Heidelberg, September 2006.

[DS08a] Hüseyin Demirci and Ali Aydin Selçuk. A meet-in-the-middle attack on 8-round AES. In Kaisa Nyberg, editor, *FSE 2008*, volume 5086 of *LNCS*, pages 116–126. Springer, Heidelberg, February 2008.

[DS08b] Itai Dinur and Adi Shamir. Cube attacks on tweakable black box polynomials. Cryptology ePrint Archive, Report 2008/385, 2008. https://eprint.iacr.org/2008/385.

[DST03] Hüseyin Demirci, Ali Aydin Selçuk, and Erkan Türe. A new meet-in-the-middle attack on the idea block cipher. In *International workshop on selected areas in cryptography*, pages 117–129. Springer, 2003.

[DTÇB09] Hüseyin Demirci, Ihsan Taskin, Mustafa Çoban, and Adnan Baysal. Improved meet-in-the-middle attacks on AES. In Bimal K. Roy and Nicolas Sendrier, editors, *INDOCRYPT 2009*, volume 5922 of *LNCS*, pages 144–156. Springer, Heidelberg, December 2009.

[EGB20] Zahra Eskandari and Abbas Ghaemi Bafghi. Cube distinguisher extraction using division property in block ciphers. *IET Information Security*, 14(1):72–80, 2020.

[EKKT19] Zahra Eskandari, Andreas Brasen Kidmose, Stefan Kölbl, and Tyge Tiessen. Finding integral distinguishers with ease. In Carlos Cid and Michael J. Jacobson Jr:, editors, *SAC 2018*, volume 11349 of *LNCS*, pages 115–138. Springer, Heidelberg, August 2019.

[ELN$^+$14] Sareh Emami, San Ling, Ivica Nikolic, Josef Pieprzyk, and Huaxiong Wang. Low probability differentials and the cryptanalysis of full-round CLEFIA-128. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part I*, volume 8873 of *LNCS*, pages 141–157. Springer, Heidelberg, December 2014.

[Fau99] Jean-Charles Faugere. A new efficient algorithm for computing gröbner bases (f4). *Journal of pure and applied algebra*, 139(1-3):61–88, 1999.

[Fau02] Jean Charles Faugere. A new efficient algorithm for computing gröbner bases without reduction to zero (f 5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 75–83, 2002.

[Fer99] Niels Ferguson. Impossible differentials in twofish. *Counterpane Systems. October*, 19, 1999.

[FGL09] Ewan Fleischmann, Michael Gorski, and Stefan Lucks. Attacking 9 and 10 rounds of AES-256. In Colin Boyd and Juan Manuel González Nieto, editors, *ACISP 09*, volume 5594 of *LNCS*, pages 60–72. Springer, Heidelberg, July 2009.

[FJP13] Pierre-Alain Fouque, Jérémy Jean, and Thomas Peyrin. Structural evaluation of AES and chosen-key distinguisher of 9-round AES-128. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 183–203. Springer, Heidelberg, August 2013.

[FKL$^+$01] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 213–230. Springer, Heidelberg, April 2001.

[FSW01] Niels Ferguson, Richard Schroeppel, and Doug Whiting. A simple algebraic representation of Rijndael. In Serge Vaudenay and Amr M. Youssef, editors, *SAC 2001*, volume 2259 of *LNCS*, pages 103–111. Springer, Heidelberg, August 2001.

[GC90] Henri Gilbert and Guy Chassé. A statistical attack of the feal-8 cryptosystem. In *Conference on the Theory and Application of Cryptography*, pages 22–33. Springer, 1990.

[GHJV00] Henri Gilbert, Helena Handschuh, Antoine Joux, and Serge Vaudenay. A statistical attack on rc6. In *International Workshop on Fast Software Encryption*, pages 64–74. Springer, 2000.

[Gho17] Riddhi Ghosal. Analysing relations involving small number of monomials in AES S- box. Cryptology ePrint Archive, Report 2017/580, 2017. `https://eprint.iacr.org/2017/580`.

[GJNS14] Jian Guo, Jérémy Jean, Ivica Nikolić, and Yu Sasaki. Meet-in-the-middle attacks on generic feistel constructions. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 458–477. Springer, 2014.

[GKL+11] Michael Gorski, Thomas Knapke, Eik List, Stefan Lucks, and Jakob Wenzel. Mars attacks! revisited - differential attack on 12 rounds of the MARS core and defeating the complex MARS key-schedule. In Daniel J. Bernstein and Sanjit Chatterjee, editors, *INDOCRYPT 2011*, volume 7107 of *LNCS*, pages 94–113. Springer, Heidelberg, December 2011.

[GL08] Michael Gorski and Stefan Lucks. New related-key boomerang attacks on AES. In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, *INDOCRYPT 2008*, volume 5365 of *LNCS*, pages 266–278. Springer, Heidelberg, December 2008.

[GLR+19] Lorenzo Grassi, Gregor Leander, Christian Rechberger, Cihangir Tezcan, and Friedrich Wiemer. Weak-key subspace trails and applications to AES. Cryptology ePrint Archive, Report 2019/852, 2019. `https://eprint.iacr.org/2019/852`.

[GM00] Henri Gilbert and Marine Minier. A collision attack on 7 rounds of rijndael. In *AES candidate conference*, volume 230, page 241. New York, 2000.

[Gra17] Lorenzo Grassi. Structural truncated differential attacks on round-reduced AES. Cryptology ePrint Archive, Report 2017/832, 2017. `https://eprint.iacr.org/2017/832`.

[Gra18] Lorenzo Grassi. Mixture differential cryptanalysis: a new approach to distinguishers and attacks on round-reduced aes. *IACR Transactions on Symmetric Cryptology*, pages 133–160, 2018.

[Gra19] Lorenzo Grassi. Probabilistic mixture differential cryptanalysis on round-reduced AES. In Kenneth G. Paterson and Douglas Stebila, editors, *SAC 2019*, volume 11959 of *LNCS*, pages 53–84. Springer, Heidelberg, August 2019.

[GRR16] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. Subspace trail cryptanalysis and its applications to aes. *Cryptology ePrint Archive*, 2016.

[GRR17] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. A new structural-differential property of 5-round AES. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part II*, volume 10211 of *LNCS*, pages 289–317. Springer, Heidelberg, April / May 2017.

[GS13] David Gstir and Martin Schläffer. Fast software encryption attacks on AES. In Amr Youssef, Abderrahmane Nitaj, and Aboul Ella Hassanien, editors, *AFRICACRYPT 13*, volume 7918 of *LNCS*, pages 359–374. Springer, Heidelberg, June 2013.

[HBS20] Hosein Hadipour, Nasour Bagheri, and Ling Song. Improved rectangle attacks on SKINNY and CRAFT. Cryptology ePrint Archive, Report 2020/1317, 2020. `https://eprint.iacr.org/2020/1317`.

[HCN08] Miia Hermelin, Joo Yeon Cho, and Kaisa Nyberg. Multidimensional linear cryptanalysis of reduced round Serpent. In Yi Mu, Willy Susilo, and Jennifer Seberry, editors, *ACISP 08*, volume 5107 of *LNCS*, pages 203–215. Springer, Heidelberg, July 2008.

[Hey02] Howard M Heys. A tutorial on linear and differential cryptanalysis. *Cryptologia*, 26(3):189–221, 2002.

[HKLP05] Seokhie Hong, Jongsung Kim, Sangjin Lee, and Bart Preneel. Related-key rectangle attacks on reduced versions of SHACAL-1 and AES-192. In Henri Gilbert and Helena Handschuh, editors, *FSE 2005*, volume 3557 of *LNCS*, pages 368–383. Springer, Heidelberg, February 2005.

[HM97] Carlo Harpes and James L. Massey. Partitioning cryptanalysis. In Eli Biham, editor, *FSE'97*, volume 1267 of *LNCS*, pages 13–27. Springer, Heidelberg, January 1997.

[HQ01] Yeping He and Sihan Qing. Square attack on reduced Camellia cipher. In Sihan Qing, Tatsuaki Okamoto, and Jianying Zhou, editors, *ICICS 01*, volume 2229 of *LNCS*, pages 238–245. Springer, Heidelberg, November 2001.

[HR10] Viet Tung Hoang and Phillip Rogaway. On generalized feistel networks. In *Annual Cryptology Conference*, pages 613–630. Springer, 2010.

[HSK03] Yasuo Hatano, Hiroki Sekine, and Toshinobu Kaneko. Higher order differential attack of Camellia (II). In Kaisa Nyberg and Howard M. Heys, editors, *SAC 2002*, volume 2595 of *LNCS*, pages 129–146. Springer, Heidelberg, August 2003.

[JD04] Goce Jakimoski and Yvo Desmedt. Related-key differential cryptanalysis of 192-bit key AES variants. In Mitsuru Matsui and Robert J. Zuccherato, editors, *SAC 2003*, volume 3006 of *LNCS*, pages 208–221. Springer, Heidelberg, August 2004.

[JK97] Thomas Jakobsen and Lars R. Knudsen. The interpolation attack on block ciphers. In Eli Biham, editor, *FSE'97*, volume 1267 of *LNCS*, pages 28–40. Springer, Heidelberg, January 1997.

[JK01] Thomas Jakobsen and Lars R. Knudsen. Attacks on block ciphers of low algebraic degree. *Journal of Cryptology*, 14(3):197–210, June 2001.

[JL12] Keting Jia and Leibo Li. Improved impossible differential attacks on reduced-round MISTY1. In Dong Hoon Lee and Moti Yung, editors, *WISA 12*, volume 7690 of *LNCS*, pages 15–27. Springer, Heidelberg, August 2012.

[Jun05] Pascal Junod. Statistical cryptanalysis of block ciphers. Technical report, EPFL, 2005.

[JW16] Keting Jia and Ning Wang. Impossible differential cryptanalysis of 14-round camellia-192. In Joseph K. Liu and Ron Steinfeld, editors, *ACISP 16, Part II*, volume 9723 of *LNCS*, pages 363–378. Springer, Heidelberg, July 2016.

[JZD21] Fulei Ji, Wentao Zhang, and Tianyou Ding. Improving matsui's search algorithm for the best differential/linear trails and its applications for des, desl and gift. *The Computer Journal*, 64(4):610–627, 2021.

[Kar07] Orhun Kara. Reflection attacks on product ciphers. Cryptology ePrint Archive, Report 2007/043, 2007. https://eprint.iacr.org/2007/043.

[KHP07] Jongsung Kim, Seokhie Hong, and Bart Preneel. Related-key rectangle attacks on reduced AES-192 and AES-256. In Alex Biryukov, editor, *FSE 2007*, volume 4593 of *LNCS*, pages 225–241. Springer, Heidelberg, March 2007.

[KHP+12] Jongsung Kim, Seokhie Hong, Bart Preneel, Eli Biham, Orr Dunkelman, and Nathan Keller. Related-key boomerang and rectangle attacks: theory and experimental analysis. *IEEE transactions on information theory*, 58(7):4948–4966, 2012.

[KHS$^+$03] Jongsung Kim, Seokhie Hong, Jaechul Sung, Changhoon Lee, and Sangjin Lee. Impossible differential cryptanalysis for block cipher structures. In Thomas Johansson and Subhamoy Maitra, editors, *INDOCRYPT 2003*, volume 2904 of *LNCS*, pages 82–96. Springer, Heidelberg, December 2003.

[KID01] Kaoru Kurosawa, Tetsu Iwata, and Quang Viet Duong. Root finding interpolation attack. In Douglas R. Stinson and Stafford E. Tavares, editors, *SAC 2000*, volume 2012 of *LNCS*, pages 303–314. Springer, Heidelberg, August 2001.

[KKH$^+$04] Jongsung Kim, Guil Kim, Seokhie Hong, Sangjin Lee, and Dowon Hong. The related-key rectangle attack – application to shacal-1. In Huaxiong Wang, Josef Pieprzyk, and Vijay Varadharajan, editors, *Information Security and Privacy*, pages 123–136, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[KKS$^+$00] Tadayoshi Kohno, John Kelsey, Bruce Schneier, et al. Preliminary cryptanalysis of reduced-round serpent. In *AES candidate conference*, pages 195–211. Citeseer, 2000.

[KKS01] John Kelsey, Tadayoshi Kohno, and Bruce Schneier. Amplified boomerang attacks against reduced-round MARS and Serpent. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 75–93. Springer, Heidelberg, April 2001.

[KLPS17] Khoongming Khoo, Eugene Lee, Thomas Peyrin, and Siang Meng Sim. Human-readable proof of the related-key security of aes-128. *IACR Transactions on Symmetric Cryptology*, pages 59–83, 2017.

[KM01] Lars R. Knudsen and Willi Meier. Correlations in RC6 with a reduced number of rounds. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 94–108. Springer, Heidelberg, April 2001.

[KM02] Masayuki Kanda and Tsutomu Matsumoto. Security of Camellia against truncated differential cryptanalysis. In Mitsuru Matsui, editor, *FSE 2001*, volume 2355 of *LNCS*, pages 286–299. Springer, Heidelberg, April 2002.

[Knu95] Lars R. Knudsen. Truncated and higher order differentials. In Bart Preneel, editor, *FSE'94*, volume 1008 of *LNCS*, pages 196–211. Springer, Heidelberg, December 1995.

[Knu98] Lars Knudsen. Deal - a 128-bit block cipher. In *NIST AES Proposal*, 1998.

[Knu00] Lars R Knudsen. Trawling twofish. In *UNIV OF BERGEN, REPORT IN INFORMATICS*. Citeseer, 2000.

[KR00] Lars Knudsen and H Raddum. Linear approximations to the mars s-box. *AES Round*, 2, 2000.

[KRS12] Dmitry Khovratovich, Christian Rechberger, and Alexandra Savelieva. Bicliques for preimages: Attacks on Skein-512 and the SHA-2 family. In Anne Canteaut, editor, *FSE 2012*, volume 7549 of *LNCS*, pages 244–263. Springer, Heidelberg, March 2012.

[KSW96] John Kelsey, Bruce Schneier, and David Wagner. Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In Neal Koblitz, editor, *CRYPTO'96*, volume 1109 of *LNCS*, pages 237–251. Springer, Heidelberg, August 1996.

[KT22] Andreas B Kidmose and Tyge Tiessen. A formal analysis of boomerang probabilities. *IACR Transactions on Symmetric Cryptology*, pages 88–109, 2022.

[Küh01] Ulrich Kühn. Cryptanalysis of reduced-round MISTY. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 325–339. Springer, Heidelberg, May 2001.

[Küh02] Ulrich Kühn. Improved cryptanalysis of MISTY1. In Joan Daemen and Vincent Rijmen, editors, *FSE 2002*, volume 2365 of *LNCS*, pages 61–75. Springer, Heidelberg, February 2002.

[KW02] Lars R. Knudsen and David Wagner. Integral cryptanalysis. In Joan Daemen and Vincent Rijmen, editors, *FSE 2002*, volume 2365 of *LNCS*, pages 112–127. Springer, Heidelberg, February 2002.

[L$^+$00] Stefan Lucks et al. Attacking seven rounds of rijndael under 192-bit and 256-bit keys. In *AES Candidate Conference*, volume 2000, 2000.

[LAAZ11] Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. A cryptanalysis of printcipher: the invariant subspace attack. In *Annual Cryptology Conference*, pages 206–221. Springer, 2011.

[Lai94] Xuejia Lai. Higher order derivatives and differential cryptanalysis. In *Communications and cryptography*, pages 227–233. Springer, 1994.

[LCF06] Duo Lei, Li Chao, and Keqin Feng. New observation on Camellia. In Bart Preneel and Stafford Tavares, editors, *SAC 2005*, volume 3897 of *LNCS*, pages 51–64. Springer, Heidelberg, August 2006.

[LCJ11] Leibo Li, Jiazhe Chen, and Keting Jia. New impossible differential cryptanalysis of reduced-round Camellia. In Dongdai Lin, Gene Tsudik, and Xiaoyun Wang, editors, *CANS 11*, volume 7092 of *LNCS*, pages 26–39. Springer, Heidelberg, December 2011.

[LCW11] Leibo Li, Jiazhe Chen, and Xiaoyun Wang. Security of reduced-round Camellia against impossible differential attack. Cryptology ePrint Archive, Report 2011/524, 2011. `https://eprint.iacr.org/2011/524`.

[LDKK08] Jiqiang Lu, Orr Dunkelman, Nathan Keller, and Jongsung Kim. New impossible differential attacks on AES. In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, *INDOCRYPT 2008*, volume 5365 of *LNCS*, pages 279–293. Springer, Heidelberg, December 2008.

[LGL$^+$11] Ya Liu, Dawu Gu, Zhiqiang Liu, Wei Li, and Ying Man. Improved results on impossible differential cryptanalysis of reduced-round Camellia-192/256. Cryptology ePrint Archive, Report 2011/671, 2011. `https://eprint.iacr.org/2011/671`.

[LGLL12] Ya Liu, Dawu Gu, Zhiqiang Liu, and Wei Li. Improved impossible differential attack on reduced version of Camellia-192/256. Cryptology ePrint Archive, Report 2012/594, 2012. `https://eprint.iacr.org/2012/594`.

[LGZL10] Zhiqiang Liu, Dawu Gu, Jing Zhang, and Wei Li. Differential-multiple linear cryptanalysis. In Feng Bao, Moti Yung, Dongdai Lin, and Jiwu Jing, editors, *Information Security and Cryptology*, pages 35–49, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[LH94] Susan K. Langford and Martin E. Hellman. Differential-linear cryptanalysis. In Yvo Desmedt, editor, *CRYPTO'94*, volume 839 of *LNCS*, pages 17–25. Springer, Heidelberg, August 1994.

[LHL+02] Changhoon Lee, Deukjo Hong, Sungjae Lee, Sangjin Lee, Hyung-Jin Yang, and Jongin Lim. A chosen plaintext linear attack on block cipher CIKS-1. In Robert H. Deng, Sihan Qing, Feng Bao, and Jianying Zhou, editors, *ICICS 02*, volume 2513 of *LNCS*, pages 456–468. Springer, Heidelberg, December 2002.

[LJ14] Leibo Li and Keting Jia. Improved meet-in-the-middle attacks on reduced-round Camellia-192/256. Cryptology ePrint Archive, Report 2014/292, 2014. https://eprint.iacr.org/2014/292.

[LJW15] Leibo Li, Keting Jia, and Xiaoyun Wang. Improved single-key attacks on 9-round AES-192/256. In Carlos Cid and Christian Rechberger, editors, *FSE 2014*, volume 8540 of *LNCS*, pages 127–146. Springer, Heidelberg, March 2015.

[LJWD15] Leibo Li, Keting Jia, Xiaoyun Wang, and Xiaoyang Dong. Meet-in-the-middle technique for truncated differential and its applications to CLEFIA and Camellia. In Gregor Leander, editor, *FSE 2015*, volume 9054 of *LNCS*, pages 48–70. Springer, Heidelberg, March 2015.

[LK07] Chu-Wee Lim and Khoongming Khoo. An analysis of XSL applied to BES. In Alex Biryukov, editor, *FSE 2007*, volume 4593 of *LNCS*, pages 242–253. Springer, Heidelberg, March 2007.

[LKKD08] Jiqiang Lu, Jongsung Kim, Nathan Keller, and Orr Dunkelman. Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1. In Tal Malkin, editor, *CT-RSA 2008*, volume 4964 of *LNCS*, pages 370–386. Springer, Heidelberg, April 2008.

[LLF08] Duo Lei, Chao Li, and Keqin Feng. Square like attack on Camellia. In Sihan Qing, Hideki Imai, and Guilin Wang, editors, *ICICS 07*, volume 4861 of *LNCS*, pages 269–283. Springer, Heidelberg, December 2008.

[LLG+12] Ya Liu, Leibo Li, Dawu Gu, Xiaoyun Wang, Zhiqiang Liu, Jiazhe Chen, and Wei Li. New observations on impossible differential cryptanalysis of reduced-round Camellia. In Anne Canteaut, editor, *FSE 2012*, volume 7549 of *LNCS*, pages 90–109. Springer, Heidelberg, March 2012.

[LLSS10] Ruilin Li, Chao Li, Jinshu Su, and Bing Sun. Security evaluation of MISTY structure with SPN round function. Cryptology ePrint Archive, Report 2010/661, 2010. https://eprint.iacr.org/2010/661.

[LP19] Chaoyun Li and Bart Preneel. Improved interpolation attacks on cryptographic primitives of low algebraic degree. In Kenneth G. Paterson and Douglas Stebila, editors, *SAC 2019*, volume 11959 of *LNCS*, pages 171–193. Springer, Heidelberg, August 2019.

[LP21] Gaëtan Leurent and Clara Pernot. New representations of the AES key schedule. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part I*, volume 12696 of *LNCS*, pages 54–84. Springer, Heidelberg, October 2021.

[LR88] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17(2), 1988.

[Lu10a] Jiqiang Lu. Differential attack on five rounds of the SC2000 block cipher. Cryptology ePrint Archive, Report 2010/593, 2010. `https://eprint.iacr.org/2010/593`.

[Lu10b] Jiqiang Lu. New methodologies for differential-linear cryptanalysis and its extensions. Cryptology ePrint Archive, Report 2010/025, 2010. `https://eprint.iacr.org/2010/025`.

[Lu12] Jiqiang Lu. A methodology for differential-linear cryptanalysis and its applications - (extended abstract). In Anne Canteaut, editor, *FSE 2012*, volume 7549 of *LNCS*, pages 69–89. Springer, Heidelberg, March 2012.

[Luc02] Stefan Lucks. The saturation attack - a bait for Twofish. In Mitsuru Matsui, editor, *FSE 2001*, volume 2355 of *LNCS*, pages 1–15. Springer, Heidelberg, April 2002.

[LWFK12] Jiqiang Lu, Yongzhuang Wei, Pierre-Alain Fouque, and Jongsung Kim. Cryptanalysis of reduced versions of the camellia block cipher. *IET Information Security*, 6(3):228–238, 2012.

[LWKP12] Jiqiang Lu, Yongzhuang Wei, Jongsung Kim, and Enes Pasalic. The higher-order meet-in-the-middle attack and its application to the Camellia block cipher. In Steven D. Galbraith and Mridul Nandi, editors, *INDOCRYPT 2012*, volume 7668 of *LNCS*, pages 244–264. Springer, Heidelberg, December 2012.

[LWLG09] Yiyuan Luo, Zhongming Wu, Xuejia Lai, and Guang Gong. A unified method for finding impossible differentials of block cipher structures. Cryptology ePrint Archive, Report 2009/627, 2009. `https://eprint.iacr.org/2009/627`.

[LWPF12] Jiqiang Lu, Yongzhuang Wei, Enes Pasalic, and Pierre-Alain Fouque. Meet-in-the-middle attack on reduced versions of the Camellia block cipher. In Goichiro Hanaoka and Toshihiro Yamauchi, editors, *IWSEC 12*, volume 7631 of *LNCS*, pages 197–215. Springer, Heidelberg, November 2012.

[LWWZ14] Li Lin, Wenling Wu, Yanfeng Wang, and Lei Zhang. General model of the single-key meet-in-the-middle distinguisher on the word-oriented block cipher. In Hyang-Sook Lee and Dong-Guk Han, editors, *ICISC 13*, volume 8565 of *LNCS*, pages 203–223. Springer, Heidelberg, November 2014.

[LWZ12] Yanjun Li, Wenling Wu, and Lei Zhang. Improved integral attacks on reduced-round CLEFIA block cipher. In Souhwan Jung and Moti Yung, editors, *WISA 11*, volume 7115 of *LNCS*, pages 28–39. Springer, Heidelberg, August 2012.

[LWZZ11] Yanjun Li, Wenling Wu, Liting Zhang, and Lei Zhang. Improved integral attacks on reduced round Camellia. Cryptology ePrint Archive, Report 2011/163, 2011. `https://eprint.iacr.org/2011/163`.

[LYW13] Jiqiang Lu, Wun-She Yap, and Yongzhuang Wei. Weak keys of the full MISTY1 block cipher for related-key differential cryptanalysis. In Ed Dawson, editor, *CT-RSA 2013*, volume 7779 of *LNCS*, pages 389–404. Springer, Heidelberg, February / March 2013.

[Mat94] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *LNCS*, pages 386–397. Springer, Heidelberg, May 1994.

[Mat95] Mitsuru Matsui. On correlation between the order of S-boxes and the strength of DES. In Alfredo De Santis, editor, *EUROCRYPT'94*, volume 950 of *LNCS*, pages 366–375. Springer, Heidelberg, May 1995.

[Mat97] Mitsuru Matsui. New block encryption algorithm MISTY. In Eli Biham, editor, *FSE'97*, volume 1267 of *LNCS*, pages 54–68. Springer, Heidelberg, January 1997.

[Mat00] Mitsuru Matsui. Supporting document of misty1 (version 1.10). `http://tnlandforms.us/cs594-cns/misty.pdf`, 2000. Accessed: 2022-05-22.

[MC13a] James McLaughlin and John A. Clark. Filtered nonlinear cryptanalysis of reduced-round Serpent, and the wrong-key randomization hypothesis. In Martijn Stam, editor, *14th IMA International Conference on Cryptography and Coding*, volume 8308 of *LNCS*, pages 120–140. Springer, Heidelberg, December 2013.

[MC13b] James McLaughlin and John A. Clark. Nonlinear cryptanalysis of reduced-round Serpent and metaheuristic search for S-box approximations. Cryptology ePrint Archive, Report 2013/022, 2013. `https://eprint.iacr.org/2013/022`.

[MDRMH10] Hamid Mala, Mohammad Dakhilalian, Vincent Rijmen, and Mahmoud Modarres-Hashemi. Improved impossible differential cryptanalysis of 7-round AES-128. In Guang Gong and Kishan Chand Gupta, editors, *INDOCRYPT 2010*, volume 6498 of *LNCS*, pages 282–291. Springer, Heidelberg, December 2010.

[MDS11] Hamid Mala, Mohammad Dakhilalian, and Mohsen Shakiba. Impossible differential attacks on 13-round clefia-128. *Journal of Computer Science and Technology*, 26(4):744–750, 2011.

[MR00] Sean Murphy and MJB Robshaw. Differential cryptanalysis, key-dependent s-boxes, and twofish. 2000.

[MR02] Sean Murphy and Matthew J. B. Robshaw. Essential algebraic structure within the AES. In Moti Yung, editor, *CRYPTO 2002*, volume 2442 of *LNCS*, pages 1–16. Springer, Heidelberg, August 2002.

[MSAK99] Shiho Moriai, Makoto Sugita, Kazumaro Aoki, and Masayuki Kanda. Security of e2 against truncated differential cryptanalysis. In Howard M. Heys and Carlisle M. Adams, editors, *SAC 1999*, volume 1758 of *LNCS*, pages 106–117. Springer, Heidelberg, August 1999.

[MSDB09] Hamid Mala, Mohsen Shakiba, Mohammad Dakhilalian, and Ghadamali Bagherikaram. New results on impossible differential cryptanalysis of reduced-round Camellia-128. In Michael J. Jacobson Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, *SAC 2009*, volume 5867 of *LNCS*, pages 281–294. Springer, Heidelberg, August 2009.

[MT99] Mitsuru Matsui and Toshio Tokita. Cryptanalysis of a reduced version of the block cipher E2. In Lars R. Knudsen, editor, *FSE'99*, volume 1636 of *LNCS*, pages 71–80. Springer, Heidelberg, March 1999.

[Mur11] Sean Murphy. The return of the cryptographic boomerang. *IEEE Transactions on Information Theory*, 57(4):2517–2521, 2011.

[MWGP12] Nicky Mouha, Qingju Wang, Dawu Gu, and Bart Preneel. Differential and linear cryptanalysis using mixed-integer linear programming. In Chuan-Kun Wu, Moti Yung, and Dongdai Lin, editors, *Information Security and Cryptology*, pages 57–76, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[MY93] Mitsuru Matsui and Atsuhiro Yamagishi. A new method for known plaintext attack of FEAL cipher. In Rainer A. Rueppel, editor, *EUROCRYPT'92*, volume 658 of *LNCS*, pages 81–91. Springer, Heidelberg, May 1993.

[MY00] Shiho Moriai and Yiqun Lisa Yin. Cryptanalysis of twofish (ii). 2000.

[NBP$^+$01] J. Nakahara Jr., P. S. L. M. Barreto, B. Preneel, J. Vandewalle, and H. Y. Kim. SQUARE attacks on reduced-round PES and IDEA block ciphers. Cryptology ePrint Archive, Report 2001/068, 2001. https://eprint.iacr.org/2001/068.

[NC02] NTT and Mitsubishi Electric Corporation. Camellia: A 128-bit block cipher suitable for multiple platforms. https://info.isl.ntt.co.jp/crypt/eng/camellia/dl/support.pdf, 2002. Accessed: 2022-05-22.

[NPT09] Valerie Nachef, Jacques Patarin, and Joana Treger. Generic attacks on Misty schemes -5 rounds is not enough-. Cryptology ePrint Archive, Report 2009/405, 2009. https://eprint.iacr.org/2009/405.

[NPT10] Valérie Nachef, Jacques Patarin, and Joana Treger. Generic attacks on Misty schemes. In Michel Abdalla and Paulo S. L. M. Barreto, editors, *LATINCRYPT 2010*, volume 6212 of *LNCS*, pages 222–240. Springer, Heidelberg, August 2010.

[NWW11] Phuong Ha Nguyen, Hongjun Wu, and Huaxiong Wang. Improving the algorithm 2 in multidimensional linear cryptanalysis. In Udaya Parampalli and Philip Hawkes, editors, *ACISP 11*, volume 6812 of *LNCS*, pages 61–74. Springer, Heidelberg, July 2011.

[Nyb95] Kaisa Nyberg. Linear approximation of block ciphers (rump session). In Alfredo De Santis, editor, *EUROCRYPT'94*, volume 950 of *LNCS*, pages 439–444. Springer, Heidelberg, May 1995.

[Nyb96] Kaisa Nyberg. Generalized feistel networks. In *International conference on the theory and application of cryptology and information security*, pages 91–104. Springer, 1996.

[OMA95] Kazuo Ohta, Shiho Moriai, and Kazumaro Aoki. Improving the search algorithm for the best linear expression. In Don Coppersmith, editor, *CRYPTO'95*, volume 963 of *LNCS*, pages 157–170. Springer, Heidelberg, August 1995.

[OMSK01] Kenji Ohkuma, Hirofumi Muratani, Fumihiko Sano, and Shin-ichi Kawamura. The block cipher Hierocrypt. In Douglas R. Stinson and Stafford E. Tavares, editors, *SAC 2000*, volume 2012 of *LNCS*, pages 72–88. Springer, Heidelberg, August 2001.

[OSSK01] Kenji Ohkuma, Hideo Shimizu, Fumihiko Sano, and Shinichi Kawamura. Security assessment of Hierocrypt and Rijndael against the differential and linear cryptanalysis (extended abstract). Cryptology ePrint Archive, Report 2001/070, 2001. https://eprint.iacr.org/2001/070.

[Pes06] Andrey Pestunov. Statistical analysis of the MARS block cipher. Cryptology ePrint Archive, Report 2006/217, 2006. https://eprint.iacr.org/2006/217.

[Pha04] Raphael C-W Phan. Impossible differential cryptanalysis of 7-round advanced encryption standard (aes). *Information processing letters*, 91(1):33–38, 2004.

[PSC⁺02] Sangwoo Park, Soo Hak Sung, Seongtaek Chee, E-Joong Yoon, and Jongin Lim. On the security of Rijndael-like structures against differential and linear cryptanalysis. In Yuliang Zheng, editor, *ASIACRYPT 2002*, volume 2501 of *LNCS*, pages 176–191. Springer, Heidelberg, December 2002.

[RBH17] Sondre Rønjom, Navid Ghaedi Bardeh, and Tor Helleseth. Yoyo tricks with AES. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 217–243. Springer, Heidelberg, December 2017.

[rGPPG07] ETSI 3rd Generation Partnership Project (3GPP). Universal mobile telecommunications system (umts); specification of the 3gpp confidentiality and integrity algorithms; document 2: Kasumi specification (3gpp ts 35.202 version 7.0.0 release 7). https://www.etsi.org/deliver/etsi_ts/135200_135299/135202/07.00.00_60/ts_135202v070000p.pdf, 2007. Accessed: 2022-05-22.

[Rim09] Anna Rimoldi. On algebraic and statistical properties of aes-like ciphers. 2009.

[RK01] Håvard Raddum and Lars R. Knudsen. A differential attack on reduced-round SC2000. In Serge Vaudenay and Amr M. Youssef, editors, *SAC 2001*, volume 2259 of *LNCS*, pages 190–198. Springer, Heidelberg, August 2001.

[RM07] MJB Robshaw and S Murphy. Comments on the security of the aes and the xsltechnique, 2007.

[RY00] MJB Robshaw and Yiqun Lisa Yin. Potential flaws in the conjectured resistance of mars to linear cryptanalysis. In *PUBLIC COMMENTS ON AES CANDIDATE ALGORITHMS—ROUND 2*. Citeseer, 2000.

[Saa99] M Saarinen. A note regarding the hash function use of mars and rc6. *available online fro m http://www. jyu. fi/˜ mjos*, 1999.

[Saa19] Markku-Juhani O. Saarinen. A chosen key attack against the secret S-boxes of GOST. Cryptology ePrint Archive, Report 2019/540, 2019. https://eprint.iacr.org/2019/540.

[SAB09] Bhupendra Singh, Lexy Alexander, and Sanjay Burman. On algebraic relations of Serpent s-boxes. Cryptology ePrint Archive, Report 2009/038, 2009. https://eprint.iacr.org/2009/038.

[Sas10] Yu Sasaki. Known-key attacks on Rijndael with large blocks and strengthening ShiftRow parameter. In Isao Echizen, Noboru Kunihiro, and Ryôichi Sasaki, editors, *IWSEC 10*, volume 6434 of *LNCS*, pages 301–315. Springer, Heidelberg, November 2010.

[Sch02] Bruce Schneier. Crypto-gram: September 15, 2002. https://www.schneier.com/crypto-gram/archives/2002/0915.html#1, 2002. Accessed: 2022-05-22.

[Sch05] Bruce Schneier. Twofish cryptanalysis rumors. https://www.schneier.com/blog/archives/2005/11/twofish_cryptan.html, 2005. Accessed: 2022-05-22.

[SGL+17] Siwei Sun, David Gerault, Pascal Lafourcade, Qianqian Yang, Yosuke Todo, Kexin Qiao, and Lei Hu. Analysis of AES, SKINNY, and others with constraint programming. *IACR Trans. Symm. Cryptol.*, 2017(1):281–306, 2017.

[SKA02] Taizo Shirai, Shoji Kanamaru, and George Abe. Improved upper bounds of differential and linear characteristic probability for Camellia. In Joan Daemen and Vincent Rijmen, editors, *FSE 2002*, volume 2365 of *LNCS*, pages 128–142. Springer, Heidelberg, February 2002.

[SKI01] Makoto Sugita, Kazukuni Kobara, and Hideki Imai. Security of reduced version of the block cipher Camellia against truncated and impossible differential cryptanalysis. In Colin Boyd, editor, *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 193–207. Springer, Heidelberg, December 2001.

[SKW+98] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. Twofish: A 128-bit block cipher. https://www.schneier.com/wp-content/uploads/2016/02/paper-twofish-paper.pdf, 1998. Accessed: 2022-05-22.

[SKW+99] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, and Chris Hall. On the Twofish key schedule. In Stafford E. Tavares and Henk Meijer, editors, *SAC 1998*, volume 1556 of *LNCS*, pages 27–42. Springer, Heidelberg, August 1999.

[SL09] Xiaorui Sun and Xuejia Lai. Improved integral attacks on MISTY1. In Michael J. Jacobson Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, *SAC 2009*, volume 5867 of *LNCS*, pages 266–280. Springer, Heidelberg, August 2009.

[SLG+16] Bing Sun, Meicheng Liu, Jian Guo, Vincent Rijmen, and Ruilin Li. Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 196–213. Springer, Heidelberg, May 2016.

[SLR+15] Bing Sun, Zhiqiang Liu, Vincent Rijmen, Ruilin Li, Lei Cheng, Qingju Wang, Hoda Alkhzaimi, and Chao Li. Links among impossible differential, integral and zero correlation linear cryptanalysis. Cryptology ePrint Archive, Report 2015/181, 2015. https://eprint.iacr.org/2015/181.

[Son07] The 128-bit blockcipher CLEFIA security and performance evaluations revision 1.0. https://www.sony.net/Products/cryptography/clefia/download/data/clefia-eval-1.0.pdf, 2007. Accessed: 2022-05-22.

[SQH19] Ling Song, Xianrui Qin, and Lei Hu. Boomerang connectivity table revisited. *IACR Trans. Symm. Cryptol.*, 2019(1):118–141, 2019.

[SSA$^+$07] Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-bit blockcipher CLEFIA (extended abstract). In Alex Biryukov, editor, *FSE 2007*, volume 4593 of *LNCS*, pages 181–195. Springer, Heidelberg, March 2007.

[SSD$^+$18] Danping Shi, Siwei Sun, Patrick Derbez, Yosuke Todo, Bing Sun, and Lei Hu. Programming the Demirci-Selçuk meet-in-the-middle attack with constraints. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 3–34. Springer, Heidelberg, December 2018.

[ST16] Yu Sasaki and Yosuke Todo. New impossible differential search tool from design and cryptanalysis aspects. Cryptology ePrint Archive, Report 2016/1181, 2016. https://eprint.iacr.org/2016/1181.

[SW13] Yu Sasaki and Lei Wang. Meet-in-the-middle technique for integral attacks against Feistel ciphers. In Lars R. Knudsen and Huapeng Wu, editors, *SAC 2012*, volume 7707 of *LNCS*, pages 234–251. Springer, Heidelberg, August 2013.

[SYY$^+$02] Takeshi Shimoyama, Hitoshi Yanami, Kazuhiro Yokoyama, Masahiko Takenaka, Kouichi Itoh, Jun Yajima, Naoya Torii, and Hidema Tanaka. The block cipher SC2000. In Mitsuru Matsui, editor, *FSE 2001*, volume 2355 of *LNCS*, pages 312–327. Springer, Heidelberg, April 2002.

[TBD08] Minh Triet Tran, Doan Khanh Bui, and Anh Duc Duong. Gray s-box for advanced encryption standard. In *2008 international conference on computational intelligence and security*, volume 1, pages 253–258. IEEE, 2008.

[Tez10] Cihangir Tezcan. The improbable differential attack: Cryptanalysis of reduced round CLEFIA. In Guang Gong and Kishan Chand Gupta, editors, *INDOCRYPT 2010*, volume 6498 of *LNCS*, pages 197–209. Springer, Heidelberg, December 2010.

[THK99] Hidema Tanaka, Kazuyuki Hisamatsu, and Toshinobu Kaneko. Strength of isty1 without fl function for higher order differential attack. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 221–230. Springer, 1999.

[THSK08] Hidema Tanaka, Yasuo Hatano, Nobuyuki Sugio, and Toshinobu Kaneko. Security analysis of MISTY1. In Sehun Kim, Moti Yung, and Hyung-Woo Lee, editors, *WISA 07*, volume 4867 of *LNCS*, pages 215–226. Springer, Heidelberg, August 2008.

[Tie16] Tyge Tiessen. Polytopic cryptanalysis. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 214–239. Springer, Heidelberg, May 2016.

[TIHM17] Yosuke Todo, Takanori Isobe, Yonglin Hao, and Willi Meier. Cube attacks on non-blackbox polynomials based on division property. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part III*, volume 10403 of *LNCS*, pages 250–279. Springer, Heidelberg, August 2017.

[TLS19] Yosuke Todo, Gregor Leander, and Yu Sasaki. Nonlinear invariant attack: Practical attack on full scream, iscream, and midori64. *Journal of Cryptology*, 32(4):1383–1422, 2019.

[TM16] Yosuke Todo and Masakatu Morii. Bit-based division property and application to simon family. In Thomas Peyrin, editor, *FSE 2016*, volume 9783 of *LNCS*, pages 357–377. Springer, Heidelberg, March 2016.

[TMA14] Bungo Taga, Shiho Moriai, and Kazumaro Aoki. Differential and impossible differential related-key attacks on Hierocrypt-L1. In Willy Susilo and Yi Mu, editors, *ACISP 14*, volume 8544 of *LNCS*, pages 17–33. Springer, Heidelberg, July 2014.

[TÖ14] Cihangir Tezcan and Ferruh Özbudak. Differential factors: Improved attacks on SERPENT. Cryptology ePrint Archive, Report 2014/860, 2014. `https://eprint.iacr.org/2014/860`.

[Tod15a] Yosuke Todo. Integral cryptanalysis on full MISTY1. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 413–432. Springer, Heidelberg, August 2015.

[Tod15b] Yosuke Todo. Structural evaluation by generalized integral property. Cryptology ePrint Archive, Report 2015/090, 2015. `https://eprint.iacr.org/2015/090`.

[TSLL11] Xuehai Tang, Bing Sun, Ruilin Li, and Chao Li. Impossible differential cryptanalysis of 13-round clefia-128. *Journal of Systems and Software*, 84(7):1191–1196, 2011.

[TSSK09] Yukiyasu Tsunoo, Teruo Saito, Maki Shigeri, and Takeshi Kawabata. Higher order differential attacks on reduced-round MISTY1. In Pil Joong Lee and Jung Hee Cheon, editors, *ICISC 08*, volume 5461 of *LNCS*, pages 415–431. Springer, Heidelberg, December 2009.

[TTD14] Cihangir Tezcan, Halil Kemal Taşkın, and Murat Demircioğlu. Improbable differential attacks on serpent using undisturbed bits. In *Proceedings of the 7th International Conference on Security of Information and Networks*, pages 145–150, 2014.

[TTS$^+$08a] Yukiyasu Tsunoo, Etsuko Tsujihara, Maki Shigeri, Teruo Saito, Tomoyasu Suzaki, and Hiroyasu Kubo. Impossible differential cryptanalysis of CLEFIA. In Kaisa Nyberg, editor, *FSE 2008*, volume 5086 of *LNCS*, pages 398–411. Springer, Heidelberg, February 2008.

[TTS$^+$08b] Yukiyasu Tsunoo, Etsuko Tsujihara, Maki Shigeri, Tomoyasu Suzaki, and Takeshi Kawabata. Cryptanalysis of clefia using multiple impossible differentials. In *2008 International Symposium on Information Theory and Its Applications*, pages 1–6. IEEE, 2008.

[Tun12] Michael Tunstall. Improved "partial sums-based square attack on AES. Cryptology ePrint Archive, Report 2012/280, 2012. `https://eprint.iacr.org/2012/280`.

[TW15] Biaoshuai Tao and Hongjun Wu. Improving the biclique cryptanalysis of AES. In Ernest Foo and Douglas Stebila, editors, *ACISP 15*, volume 9144 of *LNCS*, pages 39–56. Springer, Heidelberg, June / July 2015.

[Vau96] Serge Vaudenay. An experiment on DES statistical cryptanalysis. In Li Gong and Jacques Stern, editors, *ACM CCS 96*, pages 139–147. ACM Press, March 1996.

[Vau00a] Serge Vaudenay. Chapter 3 : HIEROCRYPT-L1. https://www.cryptrec.go.jp/exreport/cryptrec-ex-1080-2000.pdf, 2000. Accessed: 2022-05-22.

[Vau00b] Serge Vaudenay. Chapter 4 : MISTY1. https://www.cryptrec.go.jp/exreport/cryptrec-ex-1081-2000.pdf, 2000. Accessed: 2022-05-22.

[Vau03] Serge Vaudenay. Decorrelation: A theory for block cipher security. *Journal of Cryptology*, 16(4):249–286, September 2003.

[VTJ14] Henk CA Van Tilborg and Sushil Jajodia. *Encyclopedia of cryptography and security*. Springer Science & Business Media, 2014.

[Wag99] David Wagner. The boomerang attack. In Lars R. Knudsen, editor, *FSE'99*, volume 1636 of *LNCS*, pages 156–170. Springer, Heidelberg, March 1999.

[WF03] Wen-Ling Wu and Deng-Guo Feng. Collision attack on reduced-round Camellia. Cryptology ePrint Archive, Report 2003/135, 2003. https://eprint.iacr.org/2003/135.

[WF04] Wenling Wu and Dengguo Feng. Differential-linear cryptanalysis of camellia. In *Progress on Cryptography*, pages 173–180. Springer, 2004.

[WFC04] Wenling Wu, Dengguo Feng, and Hua Chen. Collision attack and pseudorandomness of reduced-round Camellia. In Helena Handschuh and Anwar Hasan, editors, *SAC 2004*, volume 3357 of *LNCS*, pages 252–266. Springer, Heidelberg, August 2004.

[WHC+00] XY Wang, LCK Hui, KP Chow, CF Chong, WW Tsang, and HW Chan. The differential cryptanalysis of an aes finalist-serpent. *Technical Report TR-2000- 04*, 2000.

[WLH10] Yongzhuang Wei, Jiqiang Lu, and Yupu Hu. Meet-in-the-middle attack on 8 rounds of the AES block cipher under 192 key bits. Cryptology ePrint Archive, Report 2010/537, 2010. https://eprint.iacr.org/2010/537.

[WP19] Haoyang Wang and Thomas Peyrin. Boomerang switch in multiple rounds. application to aes variants and deoxys. *IACR Transactions on Symmetric Cryptology*, 2019(1):142–169, Mar. 2019.

[WSTP12] Meiqin Wang, Yue Sun, Elmar Tischhauser, and Bart Preneel. A model for structure attacks, with applications to PRESENT and Serpent. In Anne Canteaut, editor, *FSE 2012*, volume 7549 of *LNCS*, pages 49–68. Springer, Heidelberg, March 2012.

[WW07] Wei Wang and Xiaoyun Wang. Improved impossible differential cryptanalysis of CLEFIA. Cryptology ePrint Archive, Report 2007/466, 2007. https://eprint.iacr.org/2007/466.

[WW08] Wang Wei and Xiao-yun WANG. Saturation cryptanalysis of clefia. *Journal on Communications*, 29(10):88, 2008.

[WW10] Gaoli Wang and Shaohui Wang. Improved differential cryptanalysis of serpent. In *2010 International Conference on Computational Intelligence and Security*, pages 367–371. IEEE, 2010.

[WW11] Shengbao Wu and Mingsheng Wang. Security evaluation against differential cryptanalysis for block cipher structures. Cryptology ePrint Archive, Report 2011/551, 2011. https://eprint.iacr.org/2011/551.

[WW12] Shengbao Wu and Mingsheng Wang. Automatic search of truncated impossible differentials for word-oriented block ciphers. In Steven D. Galbraith and Mridul Nandi, editors, *INDOCRYPT 2012*, volume 7668 of *LNCS*, pages 283–302. Springer, Heidelberg, December 2012.

[WWH10] MeiQin Wang, XiaoYun Wang, and Lucas CK Hui. Differential-algebraic cryptanalysis of reduced-round of serpent-256. *Science China Information Sciences*, 53(3):546–556, 2010.

[XZBL16] Zejun Xiang, Wentao Zhang, Zhenzhen Bao, and Dongdai Lin. Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers. Cryptology ePrint Archive, Report 2016/857, 2016. `https://eprint.iacr.org/2016/857`.

[YC14] Wentan Yi and Shaozhen Chen. Multidimensional zero-correlation linear attacks on reduced-round misty1. *CoRR, abs/1410.4312*, 2014.

[YC16] Wentan Yi and Shaozhen Chen. Improved integral and zero-correlation linear cryptanalysis of reduced-round CLEFIA block cipher. Cryptology ePrint Archive, Report 2016/149, 2016. `https://eprint.iacr.org/2016/149`.

[YCC04] Bo-Yin Yang, Jiun-Ming Chen, and Nicolas Courtois. On asymptotic security estimates in XL and Gröbner bases-related algebraic cryptanalysis. In Javier López, Sihan Qing, and Eiji Okamoto, editors, *ICICS 04*, volume 3269 of *LNCS*, pages 401–413. Springer, Heidelberg, October 2004.

[YG01] Amr M. Youssef and Guang Gong. On the interpolation attacks on block ciphers. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 109–120. Springer, Heidelberg, April 2001.

[YLL13] Zheng Yuan, Xian Li, and Haixia Liu. Impossible differential-linear cryptanalysis of reduced-round CLEFIA-128. Cryptology ePrint Archive, Report 2013/301, 2013. `https://eprint.iacr.org/2013/301`.

[YPK02] Yongjin Yeom, Sangwoo Park, and Iljun Kim. On the security of CAMELLIA against the Square attack. In Joan Daemen and Vincent Rijmen, editors, *FSE 2002*, volume 2365 of *LNCS*, pages 89–99. Springer, Heidelberg, February 2002.

[YSD02] Hitoshi Yanami, Takeshi Shimoyama, and Orr Dunkelman. Differential and linear cryptanalysis of a reduced-round SC2000. In Joan Daemen and Vincent Rijmen, editors, *FSE 2002*, volume 2365 of *LNCS*, pages 34–48. Springer, Heidelberg, February 2002.

[ZCX17] Kaixin Zhao, Jie Cui, and Zhiqiang Xie. Algebraic cryptanalysis scheme of aes-256 using gröbner basis. *Journal of Electrical and Computer Engineering*, 2017, 2017.

[ZWF07] Wentao Zhang, Wenling Wu, and Dengguo Feng. New results on impossible differential cryptanalysis of reduced AES. In Kil-Hyun Nam and Gwangsoo Rhee, editors, *ICISC 07*, volume 4817 of *LNCS*, pages 239–250. Springer, Heidelberg, November 2007.

[ZWZF07] Wentao Zhang, Wenling Wu, Lei Zhang, and Dengguo Feng. Improved related-key impossible differential attacks on reduced-round AES-192. In Eli Biham and Amr M. Youssef, editors, *SAC 2006*, volume 4356 of *LNCS*, pages 15–27. Springer, Heidelberg, August 2007.

[ZZWF07] Wentao Zhang, Lei Zhang, Wenling Wu, and Dengguo Feng. Related-key differential-linear attacks on reduced AES-192. In K. Srinathan, C. Pandu Rangan, and Moti Yung, editors, *INDOCRYPT 2007*, volume 4859 of *LNCS*, pages 73–85. Springer, Heidelberg, December 2007.