Exploring the Optimal Differential Characteristics of SM4 (Full Version)

Improving Automatic Search by Including Human Insights

Bingqing Li[1,2] and Ling Sun(✉)[1,2,3]

[1] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China
[2] School of Cyber Science and Technology, Shandong University, Qingdao, China
[3] Quan Cheng Shandong Laboratory, Jinan, China
lingsun@sdu.edu.cn

Abstract. This study aims to determine the complete and precise differential properties of SM4, which have remained unknown for over twenty years after the cipher was initially released. A Boolean Satisfiability Problem (SAT) based automatic search approach is employed to achieve the objective. To improve the limited efficiency of the search focused on differential probabilities, we want to investigate the feasibility of integrating human expertise into an automatic approach to enhance the search speed. This study presents the construction of four new SAT models that describe the human-identified specific properties of short differential characteristics. All of these models are integrated into the fundamental model, and the SAT solver is implemented to assess the acceleration capabilities of the new models. The experimental results indicate that including three new models effectively decreases the overall execution time of the SAT solver. Using the novel models, we obtain the first precise minimal values for the number of active S-boxes of SM4 under single-key (complete rounds) and related-key (1-round to 19-round) settings. The first precise upper bound for differential probabilities of SM4 (1-round to 20-round) is also determined. In addition, we present the first publicly revealed optimal 19-round differential characteristic of SM4.

Keywords: Differential characteristic · Automatic search · SM4.

1 Introduction

SMS4, also called the Chinese National Encryption Algorithm or GB/T 32907-2016, is a symmetric block cipher standard China devised for secure data encryption. China's State Cryptography Administration declassified it in 2006 ([7] gives an English translation), and it became the first Chinese commercial block cipher standard in 2012 with the new name SM4. It is employed in various sectors, such as finance, government, and telecommunications. In 2016, SM4 was adopted as a national standard in China and has been incorporated into numerous international standards, including ISO/IEC 18033-3:2010 for block ciphers.

Given its importance in commercial and governmental communications, SM4 has been the subject of considerable cryptanalytic effort. Like many modern block ciphers, SM4 is designed to resist differential cryptanalysis, one of the most potent cryptanalytic methods developed by Biham and Shamir [2,3,4]. Researchers have explored various differential characteristics to find potential vulnerabilities. Su *et al.* [15] investigated the structure of SM4 and proposed several necessary conditions for short differential characteristics of the cipher. With these conditions, they found a family of 19-round differential characteristics of SM4, which included one characteristic with the largest probability of 2^{-124}.

With the introduction of the automatic method [13,12,18], the search for differential characteristics became much more accessible; many researchers attempted to use the automatic method to evaluate the differential property of SM4. Zhang *et al.* [21] exploited the Mixed Integer Linear Programming (MILP) method to determine the minimum number of active S-boxes for SM4 in the single-key and the related-key settings. They proved with the MILP optimiser that no differential characteristic with a probability larger than 2^{-128} exists for 23 rounds of SM4 in the single-key setting and 19 rounds in the related-key setting. Later, Li *et al.* [8] proposed a new method to describe the Differential Distribution Table (DDT) of large S-boxes with the MILP model. Their method was applied to SM4 for a more accurate lower bound than in [21]. Besides, they found seven new 19-round differential characteristics of SM4 with probability 2^{-124} apart from the one in [15]. Liu *et al.* [9] created an automatic model based on the Simple Theorem Prover (STP) to find optimal differential and linear characteristics for S-box-based ciphers. With the new model, they found a 19-round differential characteristic of SM4 with probability 2^{-123}. However, they cannot determine whether 2^{-123} is the upper bound of probabilities for 19-round differential characteristics of SM4. Furthermore, they withheld the specific information on the 19-round characteristic with a probability of 2^{-123}.

Nearly twenty years after the cipher was published, the exact lower bound of differential active S-boxes and the exact upper bound on differential probability for SM4 have not yet been fully determined. In this paper, we aim to fill this vacancy.

Contributions of the paper. As the Boolean Satisfiability Problem (SAT) was not used in the previous automatic search concerning SM4, we plan to implement the SAT method to conduct the search and ascertain precise bounds for SM4. We develop the fundamental SAT model to identify the differential characteristics of SM4 with the lowest number of active S-boxes and the highest differential probability. The fundamental SAT model efficiently obtains accurate lower bounds for the number of active S-boxes in both single-key and related-key settings.

Given the relatively poor performance of the search orientated to differential probabilities, we are curious whether it is possible to incorporate human insight into automatic search to accelerate the search. Before the introduction of automatic methods, cryptographers were still able to use their intuition and

experience-based heuristics to accomplish the task of looking for differential characteristics. Unique capabilities that humans possess are frequently challenging for algorithms to replicate entirely. Taking this as an inspiration, we endeavour to transform the four necessary conditions proposed by Su *et al.* [15] into Boolean formulas and develop four novel SAT models. These models are incorporated into the fundamental SAT model, and the SAT solver is employed to evaluate the acceleration capabilities of the new models. The empirical findings demonstrate that the inclusion of three novel models does reduce the total execution time of the SAT solver. Furthermore, we observe that incorporating human comprehension is of greater significance when pursuing long differential characteristics.

The differential properties of SM4 are updated with the new models. Lower bounds on the number of active S-boxes of SM4 are established in both single-key (complete rounds) and related-key (1-round to 19-round) settings. Since our search considers the whole DDT of the S-box, the new bounds are tight. The first precise upper bound for differential probabilities of SM4 (1-round to 20-round) is also derived. In addition, we determine that the upper bound of probabilities for 19-round differential characteristics is 2^{-123} and present the first publicly revealed optimal 19-round differential characteristic of SM4.

The paper's organisation is as follows. In Section 2, we will outline the preliminaries that will be utilised throughout the study and provide a description of SM4. In Section 3, the fundamental SAT model for the search for differential characteristics is developed. In Section 4, we develop new SAT models specific to four conditions of SM4's short differential characteristics to integrate human insights into automatic search. The updated findings achieved using the new models are presented in Section 5. Finally, Section 6 serves as the conclusion of the work.

2 Preliminaries

This section commences with an overview of the fundamental concept of differential cryptanalysis. Subsequently, the objective cipher of the paper, SM4, is introduced. We then recall four conditions for SM4's short differential characteristics.

2.1 Differential Cryptanalysis

Differential cryptanalysis is a cryptanalytic technique primarily used for block and stream ciphers. It focuses on the impact of *input difference* Δ_{in} on the resulting *output difference* Δ_{out} in cryptographic algorithms. Biham and Shamir [2,3,4] developed this method during the late 1980s and early 1990s. The pair of differences $(\Delta_{in}, \Delta_{out})$ is referred to as a *differential*. The *differential probability* of the differential over an n-bit primitive E_K is calculated to be

$$\Pr_{E_K}(\Delta_{in}, \Delta_{out}) = \frac{\{x \in \mathbb{F}_2^n \mid E_K(x) \oplus E_K(x \oplus \Delta_{in}) = \Delta_{out}\}}{2^n}.$$

The *weight* ω of the differential, a concept closely related to the probability of the differential, is equal to

$$\omega_{E_K}(\Delta_{in}, \Delta_{out}) = -\log_2[\Pr_{E_K}(\Delta_{in}, \Delta_{out})].$$

The process of assessing the probability of a differential to identify a valid differential for a cryptographic algorithm with multiple iterations is recognised as particularly complex. The differential is commonly localised by constructing *differential characteristics*, which facilitate the tracking of internal differences after each round. Denote $(\Delta_{in} = \Delta_0, \Delta_1, \ldots, \Delta_R = \Delta_{out})$ as an R-round differential characteristic. Assume that the R-round encryption E_K can be represented as the composition of R round functions as $E_K = F_{K_{R-1}} \circ F_{K_{R-2}} \circ \cdots \circ F_{K_0}$. Based on the assumption that the round keys K_0, K_1, ..., K_{R-1} are uniformly random and independent, the probability of the differential characteristic is

$$\Pr_{E_K}(\Delta_0, \Delta_1, \ldots, \Delta_R) = \prod_{r=0}^{R-1} \Pr_{F_{K_r}}(\Delta_r, \Delta_{r+1}).$$

S-boxes are typically the most complicated element when determining differential characteristics for round functions. In order to simplify the study of S-boxes, we commonly generate a *Differential Distribution Table* (DDT). The DDT for an s-bit S-box consists of 2^s rows and 2^s columns. The value in the i-th row and j-th column is the number of pairs that validate the differential (i, j). The S-box is *active* if its differential is associated with an element in the DDT that is strictly less than 2^s and is nonzero.

2.2 Specification of SM4

SM4 [7] is a block cipher with a block size of 128 bits and a 128-bit key. It comprises 32 rounds, and the round function's overall framework is based on an unbalanced Feistel network. Only one of the four 32-bit words is updated in each round. In the r-th round $(0 \leqslant r \leqslant 31)$, the 128-bit input state is partitioned into four 32-bit words, denoted as $X_r \| X_{r+1} \| X_{r+2} \| X_{r+3}$, and the 32-bit round key is denoted as RK_r. The r-th round's output can be represented as $X_{r+1} \| X_{r+2} \| X_{r+3} \| X_{r+4}$, where $X_{r+4} = X_r \oplus T(X_{r+1} \oplus X_{r+2} \oplus X_{r+3} \oplus RK_r)$. The transformation T consists of a nonlinear substitution S and a linear diffusion function L, represented as $T = L \circ S$. An illustration of the round function can be found in Figure 1.

Nonlinear substitution S The nonlinear transformation S applies the identical 8×8 S-box S to each byte of the 32-bit input.

Linear diffusion L The linear function L for the 32-bit input X is defined as

$$L(X) = X \oplus (X \lll 2) \oplus (X \lll 10) \oplus (X \lll 18) \oplus (X \lll 24).$$

The key schedule of SM4 is almost the same as the round function, and we omit the details. For further information, see [7].

2.3 Necessary Conditions for Differential Characteristics of SM4

Finding differential characteristics in a cipher is vital to conducting differential cryptanalysis. However, finding effective differential characteristics can be challenging and requires a deep understanding of the cipher's structure and behaviour. Su *et al.* [15] proposed four necessary conditions for short differential characteristics of SM4. In the following, we use ΔY_r and ΔZ_r to denote the input and output differences of the nonlinear substitution S in the r-th round. 0^ℓ denotes an ℓ-bit string, with each bit being zero.

Theorem 1 (Su *et al.* [15]). *The following equation holds for any 5-round differential characteristic from the r-th to the $(r+4)$-th round.*

$$\Delta X_{r+1} \oplus \Delta X_{r+2} \oplus \Delta X_{r+3} \oplus \Delta X_{r+5} \oplus \Delta X_{r+6} \oplus \Delta X_{r+7} = \Delta Y_r \oplus \Delta Y_{r+4}.$$

Theorem 2 (Su *et al.* [15]). *In a 5-round differential characteristic spanning from the r-th round to the $(r+4)$-th round, if $\Delta Y_r \neq \Delta Y_{r+4}$, there must be a minimum of five active S-boxes in the characteristic.*

Theorem 3 (Su *et al.* [15]). *For any 6-round differential characteristic from the r-th to the $(r+5)$-th round, the equation $\Delta X_{r+4} \oplus \Delta X_{r+8} = \Delta Y_{r+4} \oplus \Delta Y_{r+5}$ is valid if $\Delta Y_r = \Delta Y_{r+1} = 0^{32}$.*

Corollary 1 (Su *et al.* [15]). *For any 6-round differential characteristic from the r-th to the $(r+5)$-th round, the equation $\Delta X_{r+1} \oplus \Delta X_{r+5} = \Delta Y_r \oplus \Delta Y_{r+1}$ is valid if $\Delta Y_{r+4} = \Delta Y_{r+5} = 0^{32}$.*

With the four conditions, Su *et al.* found a family of 19-round differential characteristics of SM4. The probability of the best 19-round differential characteristic they found achieves 2^{-124}.

3 Automatic Search of Differential Characteristics

After reviewing prior research [15,21,8,9] on the search for differential characteristics of SM4, we discover that the precise lower bound of differential active S-boxes and the exact upper bound on differential probability for the cipher have yet to be thoroughly determined. Given that the Boolean Satisfiability Problem (SAT) was not employed in the previous search, we intend to employ the SAT method to conduct the search and determine precise bounds for SM4.

3.1 Boolean Satisfiability Problem

The Boolean Satisfiability Problem (SAT) is one of the central problems in theoretical computer science, especially in algorithm design, complexity theory, and artificial intelligence. It involves determining whether an assignment of truth values (`true` or `false`) to variables exists in a Boolean formula such that the formula evaluates to `true`. The formula is typically expressed in *Conjunctive*

Normal Form (CNF), in which the formula is a conjunction (AND, $\wedge$) of multiple *clauses*, and each clause is a disjunction (OR, $\vee$) of *literals* (a variable or its negation $\bar{\cdot}$).

SAT was the first problem to be proven NP-complete [6]. Identifying solutions for a given Boolean formula can be exceedingly challenging and potentially require a time commitment that increases exponentially with the input size. Highly efficient SAT solvers can handle problems involving hundreds to millions of variables and clauses. In this study, we employ the SAT solver Kissat [1] in light of its performance in international SAT competitions.

Converting the differential propagation through various components into Boolean formulas in CNF can accomplish the search for differential characteristics in SM4. Figure 1 depicts the necessary Boolean variables and models for the SAT problems of SM4, in which ΔX_r, ..., ΔX_{r+4}, ΔY_r, and ΔZ_r are 32-bit vectors and δ_r, p_r, and q_r are 4-bit vectors.

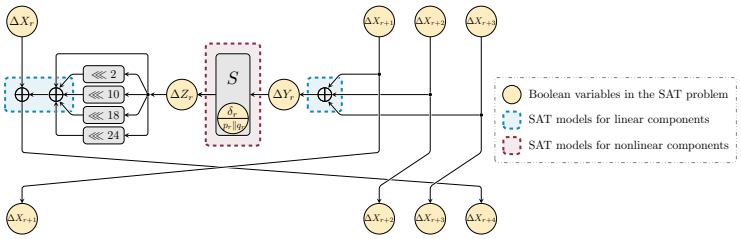


Fig. 1. Variables and models of SAT problems for SM4.

3.2 SAT Models for Linear Components of SM4

The linear components of SM4 consist of branching operations, 3-input XOR operations, and the function L. Note that the branching operation is essentially a copy operation. We can reuse the Boolean variables rather than introduce new variables and generate additional SAT models. Also, as seen in Figure 1, the function L is equivalent to a 6-input XOR operation. To characterise differential propagation over linear components of SM4, we only need the SAT model for multiple-input XOR operations. As the solver Kissat does not support Boolean formulas with XOR operations, we employ the SAT model in [17]. In order to prevent redundancy, we exclusively offer the SAT model for the 3-input XOR operation. The model for the 6-input XOR operation can be generated comparably. Below, we designate the i-th bit of an n-bit vector ΔX as $\Delta X[i]$, where $0 \leqslant i < n$.

Model 1 (3-Input XOR, [17]) *The input and output differences for the n-bit XOR operation $Y_r = X_{r+1} \oplus X_{r+2} \oplus X_{r+3}$ are denoted as ΔX_{r+1}, ΔX_{r+2}, ΔX_{r+3}, and ΔY_r, respectively. The differential propagation is valid if and only if*

ΔX_{r+1}, ΔX_{r+2}, ΔX_{r+3}, and ΔY_r validate the following equations for all 4-bit vectors $(\alpha[0], \alpha[1], \alpha[2], \alpha[3])$ with $\alpha[0] \oplus \alpha[1] \oplus \alpha[2] \oplus \alpha[3] = 1$.

$$(\Delta X_{r+1}[i] \oplus \alpha[0]) \vee \cdots \vee (\Delta X_{r+3}[i] \oplus \alpha[2]) \vee (\Delta Y_r[i] \oplus \alpha[3]) = 1, 0 \leqslant i < n.$$

Remark 1. The expressions in Model 1 are clauses in CNF, as $\Delta X_*[i] \oplus \alpha[j]$ is equal to $\Delta X_*[i]$ when $\alpha[j] = 0$ and to $\overline{\Delta X_*[i]}$ otherwise.

3.3 SAT Models for the S-box of SM4

The S-box S is the sole nonlinear component in SM4. The SAT models for S orientated to differential active S-boxes and differential probabilities are constructed using the method outlined in [16]. Sixteen Boolean variables $\Delta X = (\Delta X[0], \Delta X[1], \ldots, \Delta X[7])$ and $\Delta Y = (\Delta Y[0], \Delta Y[1], \ldots, \Delta Y[7])$ should be introduced in both models to represent S's input and output differences.

SAT model of S oriented to active S-boxes. In order to develop the SAT model focused on active S-boxes, it is necessary to include an additional Boolean variable represented as δ to indicate the activation status of the S-box. More precisely, within the prerequest that $(\Delta X, \Delta Y)$ is a possible differential, the value of δ is 1 for active S-boxes and 0 for inactive S-boxes. Next, we may construct the set,

$$\mathcal{S}_1 = \left\{ \Delta X \| \Delta Y \| \delta \;\middle|\; \begin{array}{l} \Delta X, \Delta Y \in \mathbb{F}_2^8, \delta \in \mathbb{F}_2, \mathrm{Pr}_{\mathsf{S}}(\Delta X, \Delta Y) > 0 \\ \delta = \begin{cases} 1, & \text{if } \mathrm{Pr}_{\mathsf{S}}(\Delta X, \Delta Y) < 1 \\ 0, & \text{if } \mathrm{Pr}_{\mathsf{S}}(\Delta X, \Delta Y) = 1 \end{cases} \end{array} \right\},$$

which includes all possible values for $\Delta X \| \Delta Y \| \delta$. To ensure that $\Delta X \| \Delta Y \| \delta$ only accepts values from the set $\mathcal{S}_1$, we generate a clause

$$\bigvee_{i=0}^{7} (\Delta X[i] \oplus \xi[i]) \vee \bigvee_{i=0}^{7} (\Delta Y[i] \oplus \xi[i+8]) \vee (\delta \oplus \xi[16]) = 1$$

for each 17-bit vector $\xi \notin \mathcal{S}_1$. The collection of these clauses can function as a fundamental SAT model for the S-box. Given that the set $\mathbb{F}_2^{17} \backslash \mathcal{S}_1$ contains 98686 vectors, directly employing the primary SAT model will decrease the speed of the search process. We employ the ESPRESSO[4] algorithm [5] to simplify the SAT model to reduce its size. The final SAT model orientated to active S-boxes consists of 8286 clauses. The collection of 8286 clauses is labelled as $\mathcal{C}_1$. Every element ξ' in $\mathcal{C}_1$ may be represented as a 17-bit string, where each bit $\xi'[i]$ takes values from the set $\{0, 1, *\}$. When these strings are interpreted as clauses, we specify that $\Delta X[i] \oplus \xi'[i] \equiv 1$ if $\xi'[i] = *$. In other words, when $\xi'[i] = *$, there is no restriction on the value of $\Delta X[i]$; hence, the term $\Delta X[i] \oplus \xi'[i]$ can be deleted from the clause expression. Given these symbols, the SAT model focused on active S-boxes can be formally represented in the following.

[4] The source code for the algorithm is publicly accessible at https://github.com/classabbyamp/espresso-logic.

Model 2 (Activation Status of S) *The S-box differential* $(\Delta X, \Delta Y)$ *is valid, and* δ *accurately represents* S*'s activation state, if and only if* ΔX*,* ΔY*, and* δ *verify the following equations for all 17-bit strings* ξ' *in* $\mathcal{C}_1$*.*

$$\bigvee_{i=0}^{7}(\Delta X[i] \oplus \xi'[i]) \vee \bigvee_{i=0}^{7}(\Delta Y[i] \oplus \xi'[i+8]) \vee (\delta \oplus \xi'[16]) = 1.$$

SAT model of S *oriented to probabilities.* The probability of possible differentials for the S-box S can take three values: 2^{-7}, 2^{-6}, or 1. For each S-box, we introduce two Boolean variables p and q to represent the differential probability of possible propagations. Assume that the weight of the possible propagation is $p+6q$. The 18-bit vector $\Delta X \| \Delta Y \| p \| q$ is restricted to values from the set

$$\mathcal{S}_2 = \left\{ \Delta X \| \Delta Y \| p \| q \;\middle|\; \begin{array}{l} \Delta X, \Delta Y \in \mathbb{F}_2^8, p, q \in \mathbb{F}_2, , \mathrm{Pr}_{\mathsf{S}}(\Delta X, \Delta Y) > 0 \\ p\|q = \begin{cases} 1\|1, & \text{if } \mathrm{Pr}_{\mathsf{S}}(\Delta X, \Delta Y) = 2^{-7} \\ 0\|1, & \text{if } \mathrm{Pr}_{\mathsf{S}}(\Delta X, \Delta Y) = 2^{-6} \\ 0\|0, & \text{if } \mathrm{Pr}_{\mathsf{S}}(\Delta X, \Delta Y) = 1 \end{cases} \end{array} \right\}.$$

Each vector in $\mathbb{F}_2^{18} \setminus \mathcal{S}_2$ may be interpreted as a clause, and all of these clauses together form the basic SAT model. We meticulously obtain 8599 clauses by simplifying the 229758 clauses generated by vectors in $\mathbb{F}_2^{18} \setminus \mathcal{S}_2$ using ESPRESSO. The set of the 8599 clauses is denoted as $\mathcal{C}_2$. The SAT model of the S-box orientated to differential probabilities is derived as follows.

Model 3 (Probability of S) *The differential* $(\Delta X, \Delta Y)$ *of the S-box is valid, and* $p + 6q$ *equals the weight of the differential, if and only if* ΔX*,* ΔY*,* p*, and* q *validate the following equations for all 18-bit strings* ζ *in* $\mathcal{C}_2$*.*

$$\bigvee_{i=0}^{7}(\Delta X[i] \oplus \zeta[i]) \vee \bigvee_{i=0}^{7}(\Delta Y[i] \oplus \zeta[i+8]) \vee (p \oplus \zeta[16]) \vee (q \oplus \zeta[17]) = 1.$$

3.4 SAT Model for the Objective Function

We aim to identify differential characteristics that exhibit fewer active S-boxes or high probabilities. The *cardinality inequality* $\sum_{i=0}^{\tau-1} x_i \leqslant \varpi$ may be used to abstract the objective function, where x_i $(0 \leqslant i < \tau)$ represent Boolean variables that reflect the activation status of the S-boxes or convey their differential probability. ϖ denotes a predetermined upper limit for the number of active S-boxes or the weight of the differential characteristics.

The sequential encoding method [14] can be employed to transform the cardinality inequality into clauses. Nevertheless, the sequential encoding method's direct integration will result in a sluggish searching phase, as the block size and the size of the S-box for SM4 are relatively large. Consequently, we exploit

the novel model proposed by Wang *et al.* [19], which integrates the sequential encoding method and Matsui's bounding conditions [10].

Knowledge of the lower and upper bounds of all partial sums $\sum_{i=0}^{\tau'} x_i$ $(0 \leqslant \tau' < \tau)$ is necessary for the model described in [19]. We initially implement Algorithm 1 in [19] to determine the lower bound $l_{\tau'}$ and upper bound $u_{\tau'}$ for each partial sum $\sum_{i=0}^{\tau'} x_i$. The following model can eliminate solutions that violate at least one constraint between $\sum_{i=0}^{\tau-1} x_i \leqslant \varpi$ and $l_{\tau'} \leqslant \sum_{i=0}^{\tau'} x_i \leqslant u_{\tau'}$ $(0 \leqslant \tau' < \tau)$.

Model 4 (Objective Function, [19]) *The main objective function* $\sum_{i=0}^{\tau-1} x_i \leqslant \varpi$ *requires the declaration of auxiliary Boolean variables* $\alpha_{i,j}$ $(0 \leqslant i \leqslant \tau - 2,$ $0 \leqslant j \leqslant \varpi - 1)$. *The simultaneous validity of all constraints* $\sum_{i=0}^{\tau-1} x_i \leqslant \varpi$ *and* $l_{\tau'} \leqslant \sum_{i=0}^{\tau'} x_i \leqslant u_{\tau'}$ $(0 \leqslant \tau' < \tau)$ *is ensured by the subsequent clauses.*

if $l_0 = 0$ and $u_0 = 1$ then $\overline{x_0} \vee \alpha_{0,0} = 1$
if $l_0 = u_0 = 0$ then $\overline{x_0} = 1$
if $l_0 = 1$ and $u_0 = 1$ then $x_0 = 1$
if $u_{\tau'} = 0$ then $\overline{x_{\tau'}} = 1$
if $u_{\tau'} > 0$
  if $l_{\tau'} = 0$ then $\overline{x_{\tau'}} \vee \alpha_{\tau',0} = 1$
    if $l_{\tau'-1} < u_{\tau'-1}$ then $\overline{\alpha_{\tau'-1,0}} \vee \alpha_{\tau',0} = 1$
    if $l_{\tau'-1} = j$ then
      $\overline{x_{\tau'}} \vee \alpha_{\tau',j} = 1$
    if $l_{\tau'-1} < j$ and $u_{\tau'-1} \geqslant j$ then
      $\overline{x_{\tau'}} \vee \overline{\alpha_{\tau'-1,j-1}} \vee \alpha_{\tau',j} = 1$
    if $l_{\tau'-1} \leqslant j$ and $u_{\tau'-1} \geqslant j+1$ then
      $\overline{\alpha_{\tau'-1,j}} \vee \alpha_{\tau',j} = 1$
    } $j \geqslant \max(l_{\tau'}, 1)$ and $j \leqslant u_{\tau'} - 1$
  if $u_{\tau'-1} = u_{\tau'}$ and $l_{\tau'-1} < u_{\tau'}$ then $\overline{x_{\tau'}} \vee \overline{\alpha_{\tau'-1,u_{\tau'}-1}} = 1$
  if $l_{\tau'-1} = u_{\tau'}$ then $\overline{x_{\tau'}} = 1$
} $\tau' \geqslant 1$ and $\tau' \leqslant \tau - 2$.
if $u_{\tau-1} = 0$ then $\overline{x_{\tau-1}} = 0$
if $u_{\tau-1} > 0$
  if $u_{\tau-2} = u_{\tau-1}$ and $l_{\tau-2} < u_{\tau-1}$ then $\overline{x_{\tau-1}} \vee \overline{\alpha_{\tau-2,u_{\tau-1}-1}} = 1$
  if $l_{\tau-2} = u_{\tau-1}$ then $\overline{x_{\tau-1}} = 1$

Combining all of the models in Sections 3.2 - 3.4, we can assemble SAT problems to search for differential characteristics with the fewest active S-boxes or the highest differential probability.

4 Automatic Search Enhanced by Human Insights

SM4's lower bounds for the number of active S-boxes in the single-key and related-key settings can be rapidly determined. However, the search of the SAT solver is somewhat delayed when we strive for the best differential characteristics with the highest probability. Recall that cryptographers could still utilise their intuition and experience-based heuristics when there were no automatic methods to complete the differential characteristic searching mission. The unique capabilities that humans possess are often tricky for algorithms to replicate in their totality. Therefore, we query the feasibility of integrating human insights into automatic search to enhance search performance by leveraging the collaborative synergy between human intuition and machine efficiency.

To provide a preliminary response to this question, we first convert the four conditions in Section 2.3 into SAT models. After incorporating these SAT models into the original SAT problems, we employ the SAT solver to determine whether the search for the optimal differential characteristics is accelerated.

4.1 SAT Models of Four Conditions in [15]

For the new models in this part, we keep the Boolean variables shown in Figure 1 and do not add any new ones. Theorem 1's condition is essentially a multiple-input XOR operation, making constructing its SAT model simple.

Model 5 (Theorem 1) *For any 5-round differential characteristics from the r-th to the $(r+4)$-th round, the conditions in Theorem 1 hold if and only if ΔX_{r+1}, ΔX_{r+2}, ΔX_{r+3}, ΔX_{r+5}, ΔX_{r+6}, ΔX_{r+7}, ΔY_r, and ΔY_{r+4} verify the following equations for all 8-bit vectors $(\alpha[0], \alpha[1], \ldots, \alpha[7])$ with $\bigoplus_{i=0}^{7} \alpha[i] = 1$.*

$$(\Delta X_{r+1}[i] \oplus \alpha[0]) \vee (\Delta X_{r+2}[i] \oplus \alpha[1]) \vee \cdots \vee (\Delta Y_{r+4}[i] \oplus \alpha[7]) = 1, 0 \leqslant i < n.$$

Based on the variables shown in Figure 1, the condition in Theorem 2 can be restated as follows: if $\Delta Y_r \oplus \Delta Y_{r+4} \neq 0^{32}$, then $\sum_{i=r}^{r+4} \sum_{j=0}^{3} q_i[j] \geqslant 5$. The formula $\sum_{i=r}^{r+4} \sum_{j=0}^{3} q_i[j] \geqslant 5$ is equivalent to limiting the region of the 20-bit vector $q_r \| q_{r+1} \| \cdots \| q_{r+4}$ to those with a Hamming weight of at least 5. We construct the set

$$\mathcal{S}_3 = \left\{ \eta \in \mathbb{F}_2^{20} \;\middle|\; \sum_{i=0}^{19} \eta[i] \geqslant 5 \right\}.$$

to exclude 20-bit vectors with Hamming weights less than 5. Similarly to the development of the SAT model for the S-box discussed in Section 3.3, the clauses generated by using vectors in the set $\mathbb{F}_2^{20}\backslash\mathcal{S}_3$ allow us to remove all vectors with a Hamming weight below 5. Following the simplification with ESPRESSO, we have a total of 4845 clauses. The collection of these clauses is symbolised as $\mathcal{C}_3$. In order to construct the SAT model for Theorem 2, it is sufficient to exclude all impossible values of the 84-bit vector $\Delta Y_r\|\Delta Y_{r+4}\|q_r\|\cdots\|q_{r+4}$, namely

$$\overbrace{*\cdots*\ \underbrace{0}_{k\text{-th bit}}\ *\cdots*}^{\text{32-bit string}}\|\overbrace{*\cdots*\ \underbrace{1}_{k\text{-th bit}}\ *\cdots*}^{\text{32-bit string}}\|\underbrace{\overbrace{q_r\|\cdots\|q_{r+4}}^{\text{20-bit string}}}_{\sum_{i=r}^{r+4}\sum_{j=0}^{3}q_i[j]<5}\ \text{and}$$

$$\overbrace{*\cdots*\ \underbrace{1}_{k\text{-th bit}}\ *\cdots*}^{\text{32-bit string}}\|\overbrace{*\cdots*\ \underbrace{0}_{k\text{-th bit}}\ *\cdots*}^{\text{32-bit string}}\|\underbrace{\overbrace{q_r\|\cdots\|q_{r+4}}^{\text{20-bit string}}}_{\sum_{i=r}^{r+4}\sum_{j=0}^{3}q_i[j]<5}\ \text{for all } 0\leqslant k<32.$$

Accordingly, we formulate the subsequent model.

Model 6 (Theorem 2) *The conditions in Theorem 2 are established for any 5-round differential characteristics from the r-th to the $(r+4)$-th round if and only if ΔY_r, ΔY_{r+4}, q_r, ..., and q_{r+4} validate the following equations for all 20-bit strings $\eta\in\mathcal{C}_3$.*

$$\begin{aligned}&\Delta Y_r[k]\vee\overline{\Delta Y_{r+4}[k]}\vee(q_r[0]\oplus\eta[0])\vee\cdots\vee(q_{r+4}[3]\oplus\eta[19])=1,\\&\overline{\Delta Y_r[k]}\vee\Delta Y_{r+4}[k]\vee(q_r[0]\oplus\eta[0])\vee\cdots\vee(q_{r+4}[3]\oplus\eta[19])=1,0\leqslant k<32.\end{aligned}$$

The development of SAT models of Theorem 3 and Corollary 1 is nearly identical, and we will use Theorem 3 as an illustrative case. With the Boolean variables depicted in Figure 1, the condition in Theorem 3 is reformulated as follows: if $q_r=q_{r+1}=0^4$, then $\Delta X_{r+4}\oplus\Delta X_{r+8}\oplus\Delta Y_{r+4}\oplus\Delta Y_{r+5}=0$. Therefore, every impossible value of the 136-bit vector $\Delta X_{r+4}\|\Delta X_{r+8}\|\Delta Y_{r+4}\|\Delta Y_{r+5}\|q_r\|q_{r+1}$ adheres to the form

$$\underbrace{\overbrace{*\cdots\Delta X_{r+4}[k]\cdots*}^{\text{32-bit string}}\|\overbrace{*\cdots\Delta X_{r+8}[k]\cdots*}^{\text{32-bit string}}\|\overbrace{*\cdots\Delta Y_{r+4}[k]\cdots*}^{\text{32-bit string}}\|\overbrace{*\cdots\Delta Y_{r+5}[k]\cdots*}^{\text{32-bit string}}}_{\Delta X_{r+4}[k]\oplus\Delta X_{r+8}[k]\oplus\Delta Y_{r+4}[k]\oplus\Delta Y_{r+5}[k]=1}\|0^8,$$

where $0\leqslant k<32$. Denote the set $\{\alpha\in\mathbb{F}_2^4\mid\alpha[0]\oplus\alpha[1]\oplus\alpha[2]\oplus\alpha[3]=1\}$ as $\mathcal{C}_4$. Conditions in Theorem 3 and Corollary 1 can be incorporated into the SAT problem of SM4 via the subsequent two models.

Model 7 (Theorem 3) *For any 6-round differential characteristics from the r-th to the $(r+5)$-th round, the conditions in Theorem 3 are established if and only if ΔX_{r+4}, ΔX_{r+8}, ΔY_{r+4}, ΔY_{r+5}, q_r, and q_{r+1} validate the following equations for all vectors α in $\mathcal{C}_4$.*

$$(\Delta X_{r+4}[k] \oplus \alpha[0]) \vee \cdots \vee (\Delta Y_{r+5}[k] \oplus \alpha[3]) \vee \bigvee_{i=0}^{3} (q_r[i] \vee q_{r+1}[i]) = 1, 0 \leqslant k < 32.$$

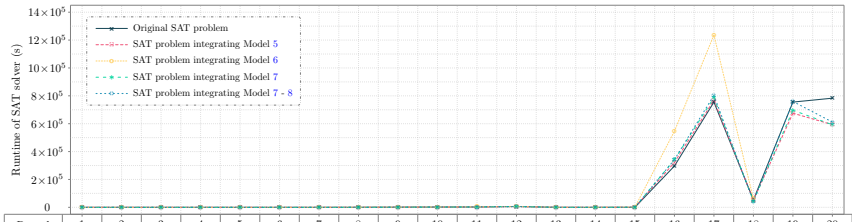
Model 8 (Corollary 1) *For any 6-round differential characteristics from the r-th to the $(r+5)$-th round, the conditions in Corollary 1 are established if and only if ΔX_{r+1}, ΔX_{r+5}, ΔY_r, ΔY_{r+1}, q_{r+4}, and q_{r+5} validate the following equations for all vectors α in $\mathcal{C}_4$.*

$$(\Delta X_{r+1}[k] \oplus \alpha[0]) \vee \cdots \vee (\Delta Y_{r+1}[k] \oplus \alpha[3]) \vee \bigvee_{i=0}^{3} (q_{r+4}[i] \vee q_{r+5}[i]) = 1, 0 \leqslant k < 32.$$

The four SAT models for the conditions suggested by Su *et al.* [15] have been formulated. Upon cursory computation, it is determined that Models 5 - 8 contain 4096, 310080, 256, and 256 clauses, respectively.

4.2 Acceleration Performance of New Models

We individually include Models 5 - 8 in the SAT problem and use the SAT solver to determine the differential characteristics of SM4 with the highest probabilities, for a range of one to twenty rounds. All the tests are implemented on a desktop with Apple M2 Ultra Processor, and the SAT solver utilises one thread. See Figure 2 for a comparison of the SAT solver's runtime.



Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Total
Original	0.1	0.1	0.2	1.5	2.1	0.4	56.9	386.4	1134.6	1906.8	2503.0	5813.4	192.1	4.6	563.8	296439	755022	53790	755124	783089	2656030.3
Model 5	0.1	0.1	0.2	1.5	2.1	0.4	62.7	343.6	1185.6	1953.4	2618.3	5802.6	252.3	5.3	572.6	321990	769053	51570	675466	593221	2424100.1
Model 6	0.1	0.1	0.2	1.5	2.1	1.6	153.9	808.1	1489.0	2363.6	3339.6	6466.8	346.2	22.5	1619.3	546503	1236181	60721	-	-	1860018.7
Model 7	0.1	0.1	0.2	1.5	2.1	0.4	50.4	325.7	1056.7	2053.6	2418.3	5880.4	160.0	8.4	650.0	341957	787009	44518	697058	592172	2475321.8
Model 7 - 8	0.1	0.1	0.2	1.5	2.1	0.4	50.3	318.3	1270.1	2185.9	2799.7	6072.2	114.7	6.5	728.9	342169	804287	39996	759609	611862	2571473.8

Fig. 2. Comparing runtime under different models.

Figure 2 illustrates that the solution time for the original SAT problem, without any additional models, is 2656030.3 seconds. However, by combining Model 5, Model 7, and Model 8, the overall runtime has been decreased to different extents. The most effective model is Model 5. In comparison to the overall runtime of the original SAT problem, the total runtime was decreased by more than 64 hours.

Model 6 exhibits the most poor performance. Within the given time constraint, the SAT problem incorporating Model 6 can only be resolved for up to 18 rounds. Furthermore, compared to other models' performance, the search phase for the initial eighteen rounds is significantly time-consuming. We hypothesise that the reason is the excessive number of clauses in Model 6. It should be noted that the original SAT problem for the search of 5-round differential characteristics includes around 200000 clauses. Consequently, the size of Model 6 exceeds the size of the original SAT problem. Incorporating these clauses will result in a considerably more complex SAT problem, thereby delaying the solver's solve phase. This finding serves as a reminder that when integrating human insights into automatic search, it is important to govern the size of the additional model within an appropriate range.

Another noteworthy finding is that the acceleration impact caused by introducing new models becomes increasingly substantial after 18 rounds. It suggests that the inclusion of human understanding is more significant in pursuing long differential characteristics, which are the necessary distinguishers in differential attacks.

5 Precise Bounds on Differential Properties of SM4

In this section, we provide the precise bounds on differential properties of SM4.

5.1 Lower Bounds on Active S-boxes in the Single-Key Setting

Since the search for the minimum active S-boxes based on the original SAT problem is very quick, we do not introduce any additional models. The runtime to get the full lower bound from 1 round to 32 rounds takes 27652.6 seconds. For comparison, as stated by Zhang *et al.* [21], obtaining the minimum number of active S-boxes for 23-round SM4 already took 36470 seconds.

Table 1 contains the full lower bound on the number of active S-boxes of SM4 in the single-key setting. Note that the newly acquired lower bounds differ from those given by Zhang *et al.* [21] beginning with the fifteenth round. Given that the MILP model in [21] assumes the S-box to be an ideal S-box and does not consider the actual DDT, the generated bounds may exhibit inaccuracies. Our SAT model can precisely describe the differential propagations of the S-box in accordance with the DDT. Thus, the newly derived bounds are precise.

5.2 Lower Bounds on Active S-boxes in the Related-Key Setting

We attempt to determine the minimum number of active S-boxes of SM4 in the related-key setting, which ranges from one round to nineteen rounds. A nonzero master key difference is enforced. The results are presented in Table 2.

Since the SAT model describes the full DDT, the search is more intricate than the one in [21]. As a result, our search is more time-consuming in certain

Table 1. Lower bounds on the number of active S-boxes in the single-key setting.

Round	Lower bounds on active S-boxes					Runtime (s)	
	Zhang *et al.* [11]	Wu *et al.* [20]	Zhang *et al.* [21]	Li *et al.* [8]	**Section 5.1**	Zhang *et al.* [21]	**Section 5.1**
1	-	0	0	0	**0**	0	**0.1**
2	-	0	0	0	**0**	0	**0.1**
3	-	0	0	0	**0**	0	**0.1**
4	-	1	1	1	**1**	0	**0.4**
5	-	2	2	2	**2**	0	**0.5**
6	-	2	2	2	**2**	0	**0.3**
7	5	5	5	5	**5**	3	**6.4**
8	6	6	6	6	**6**	6	**9.1**
9	7	7	7	7	**7**	16	**16.9**
10	8	8	8	8	**8**	23	**32.7**
11	9	8	9	9	**9**	24	**63.1**
12	10	10	10	10	**10**	22	**48.3**
13	11	10	10	10	**10**	69	**9.0**
14	11	10	10	10	**10**	75	**2.5**
15	12	12	13	12	**12**	410	**34.3**
16	13	13	14	15	**15**	395	**1092.2**
17	14	15	15	-	**16**	696	**1575.2**
18	15	15	16	-	**16**	1381	**101.5**
19	16	16	18	-	**18**	8156	**1582.3**
20	16	18	18	-	**20**	12771	**7462.8**
21	17	18	19	-	**20**	18038	**247.2**
22	18	-	20	-	**20**	24691	**22.8**
23	19	-	22	-	**23**	36470	**7248.6**
24	20	-	23	-	**24**	82857	**3251.3**
25	21	-	23	-	**25**	102451	**562.6**
26	22	-	24	-	**26**	117849	**1677.4**
27	-	-	-	-	**27**	-	**1077.1**
28	-	-	-	-	**28**	-	**307.5**
29	-	-	-	-	**29**	-	**408.6**
30	-	-	-	-	**30**	-	**379.2**
31	-	-	-	-	**31**	-	**277.4**
32	-	-	-	-	**32**	-	**155.4**

intermediate rounds than the search in [21]. Even so, our bounds maintain equivalent number of rounds to those in [21]. Furthermore, the bounds we have newly proposed are precise.

Comparing the lower bounds on active S-boxes in the related-key setting to those in the single-key setting reveals that SM4 exhibits better resistance against related-key differential attacks. Considering the complexity of SM4's key schedule, which is nearly identical to the encryption function, this outcome is not unexpected.

Table 2. Lower bounds on the number of active S-boxes in the related-key setting.

Lower bounds	Round	1	2	3	4	5	6	7	8	9	10
	Zhang *et al.* [21]	0	0	0	1	2	4	6	8	9	10
	Section 5.2	**0**	**0**	**0**	**1**	**2**	**4**	**6**	**8**	**10**	**13**
	Round	11	12	13	14	15	16	17	18	19	
	Zhang *et al.* [21]	11	13	14	14	16	18	19	20	22	
	Section 5.2	**16**	**17**	**18**	**20**	**22**	**24**	**25**	**27**	**28**	
Runtime (s)	Round	1	2	3	4	5	6	7	8	9	10
	Zhang *et al.* [21]	0	0	0	0	0	1	10	89	237	317
	Section 5.2	**0.1**	**0.2**	**0.3**	**0.9**	**1.2**	**4.5**	**18.6**	**155.8**	**1304.7**	**13636.3**
	Round	11	12	13	14	15	16	17	18	19	Total
	Zhang *et al.* [21]	757	1345	5883	27420	44492	60017	1.5 days	12 days	$<$30 days	$>$40 days
	Section 5.2	**65808.4**	**16374.1**	**10687.7**	**69346.6**	**156580**	**129159**	**0.5 days**	**1.2 days**	**0.4 days**	**7.5 days**

5.3 Upper Bounds on Probabilities in the Single-Key Setting

The upper bounds on differential probabilities of SM4 from 1 round to 20 rounds have been determined and are given in Table 3. To the best of our knowledge, we are the first to provide the whole probability bound for a maximum of 20 rounds. Evidently, the longest differential characteristic that can be employed to initiate differential attacks is 19 rounds. Liu *et al.* [9] reported the discovery of a 19-round differential characteristic with a probability of 2^{-123}. However, they cannot ensure that 2^{-123} is the maximum probability a 19-round differential characteristic can attain. We have obtained conclusive data that answer this question definitively.

Table 3. Upper bounds on probabilities in the single-key setting.

Round	1	2	3	4	5	6	7	8	9	10
Li *et al.* [8]	1	1	1	2^{-6}	2^{-12}	2^{-12}	2^{-30}	2^{-38}	2^{-46}	2^{-52}
Section 5.3	**1**	**1**	**1**	$\mathbf{2^{-6}}$	$\mathbf{2^{-12}}$	$\mathbf{2^{-12}}$	$\mathbf{2^{-30}}$	$\mathbf{2^{-38}}$	$\mathbf{2^{-46}}$	$\mathbf{2^{-52}}$
Round	11	12	13	14	15	16	17	18	19	20
Li *et al.* [8]	2^{-60}	2^{-67}	2^{-68}	2^{-68}	2^{-82}	$\geqslant 2^{-105}$	-	-	$\geqslant 2^{-124}$	-
Section 5.3	$\mathbf{2^{-60}}$	$\mathbf{2^{-67}}$	$\mathbf{2^{-68}}$	$\mathbf{2^{-68}}$	$\mathbf{2^{-82}}$	$\mathbf{2^{-101}}$	$\mathbf{2^{-110}}$	$\mathbf{2^{-111}}$	$\mathbf{2^{-123}}$	$\mathbf{2^{-130}}$

More critically, the detail of the 19-round differential characteristic was not disclosed by Liu *et al.* [9]. In Table 4, we present the 19-round differential characteristic that we identified with a probability of 2^{-123}. Notably, this is the first optimal 19-round differential characteristic of SM4 that has been publicly disclosed.

Table 4. 19-round differential characteristic of SM4 with probability 2^{-123}.

Round r	ΔX_r	ΔX_{r+1}	ΔX_{r+2}	ΔX_{r+3}	Probability
0	0x4703d247	0x263b8b26	0x479ad247	0x61835961	-
1	0x263b8b26	0x479ad247	0x61835961	0x263b8b26	2^{-6}
2	0x479ad247	0x61835961	0x263b8b26	0x4703d247	2^{-6}
3	0x61835961	0x263b8b26	0x4703d247	0x61375961	2^{-6}
4	0x263b8b26	0x4703d247	0x61375961	0x26168b26	2^{-6}
5	0x4703d247	0x61375961	0x26168b26	0x4703d247	2^{-6}
6	0x61375961	0x26168b26	0x4703d247	0x61ae5961	2^{-7}
7	0x26168b26	0x4703d247	0x61ae5961	0x26a28b26	2^{-7}
8	0x4703d247	0x61ae5961	0x26a28b26	0x472ed247	2^{-7}
9	0x61ae5961	0x26a28b26	0x472ed247	0x61ae5961	2^{-7}
10	0x26a28b26	0x472ed247	0x61ae5961	0x263b8b26	2^{-7}
11	0x472ed247	0x61ae5961	0x263b8b26	0x479ad247	2^{-7}
12	0x61ae5961	0x263b8b26	0x479ad247	0x61835961	2^{-7}
13	0x263b8b26	0x479ad247	0x61835961	0x263b8b26	2^{-7}
14	0x479ad247	0x61835961	0x263b8b26	0x4703d247	2^{-6}
15	0x61835961	0x263b8b26	0x4703d247	0x61375961	2^{-6}
16	0x263b8b26	0x4703d247	0x61375961	0x26168b26	2^{-6}
17	0x4703d247	0x61375961	0x26168b26	0x4703d247	2^{-6}
18	0x61375961	0x26168b26	0x4703d247	0x61ae5961	2^{-7}
19	0x26168b26	0x4703d247	0x61ae5961	0x479ad247	2^{-6}
Probability of the differential characteristic					2^{-123}

6 Conclusion

Given that the precise lower bounds on differential active S-boxes and the precise upper bounds on differential probability for SM4 have not yet been fully established, we intend to employ the automatic search method based on SAT problems to fill the vacancy. Firstly, we develop fundamental SAT models to search for differential characteristics with the minimum number of active S-boxes and the maximum probability. Due to the relatively sluggish search for differential characteristics with the highest probability, we endeavour to incorporate human insights into automatic search to improve search performance. Four novel models integrating human understandings have been developed to characterise the specific features of short differential characteristics. By incorporating these novel models into the initial SAT problem, the computational efficiency of the SAT solver has been increased to varying degrees. Leveraging the automatic approach, we derive the first accurate minimum values for the number of active S-boxes of SM4 under single-key (complete rounds) and related-key (1-round to 19-round) settings. The first exact upper bound for differential probabilities of

SM4 (1-round to 20-round) is also established. Furthermore, we provide the first publically disclosed optimal 19-round differential characteristic of SM4.

Acknowledgements The research leading to these results has received funding from the National Natural Science Foundation of China (Grant No. 62272273, Grant No. 62002201, Grant No. 62032014), the National Key Research and Development Program of China (Grant No. 2018YFA0704702), and the Major Basic Research Project of Natural Science Foundation of Shandong Province, China (Grant No. ZR202010220025). Ling Sun gratefully acknowledges the support by the Program of TaiShan Scholars Special Fund for young scholars (Grant No. tsqn202306043) and Xiaomi Young Talents Program.

References

1. Biere, A., Fleury, M.: Gimsatul, IsaSAT and Kissat entering the SAT Competition 2022. In: Balyo, T., Heule, M., Iser, M., Järvisalo, M., Suda, M. (eds.) Proc. of SAT Competition 2022 – Solver and Benchmark Descriptions. Department of Computer Science Series of Publications B, vol. B-2022-1, pp. 10–11. University of Helsinki (2022)
2. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. In: Menezes, A.J., Vanstone, S.A. (eds.) CRYPTO'90. LNCS, vol. 537, pp. 2–21. Springer, Berlin, Heidelberg (Aug 1991). https://doi.org/10.1007/3-540-38424-3_1
3. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology **4**(1), 3–72 (Jan 1991). https://doi.org/10.1007/BF00630563
4. Biham, E., Shamir, A.: Differential cryptanalysis of the full 16-round DES. In: Brickell, E.F. (ed.) CRYPTO'92. LNCS, vol. 740, pp. 487–496. Springer, Berlin, Heidelberg (Aug 1993). https://doi.org/10.1007/3-540-48071-4_34
5. Brayton, R.K., Hachtel, G.D., McMullen, C.T., Sangiovanni-Vincentelli, A.L.: Logic Minimization Algorithms for VLSI Synthesis, The Kluwer International Series in Engineering and Computer Science, vol. 2. Springer (1984). https://doi.org/10.1007/978-1-4613-2821-6
6. Cook, S.A.: The complexity of theorem-proving procedures. In: Harrison, M.A., Banerji, R.B., Ullman, J.D. (eds.) Proceedings of the 3rd Annual ACM Symposium on Theory of Computing, May 3-5, 1971, Shaker Heights, Ohio, USA. pp. 151–158. ACM (1971). https://doi.org/10.1145/800157.805047
7. Diffie, W., (translators), G.L.: SMS4 encryption algorithm for wireless networks. Cryptology ePrint Archive, Report 2008/329 (2008), https://eprint.iacr.org/2008/329
8. Li, L., Wu, W., Zhang, L., Zheng, Y.: New method to describe the differential distribution table for large S-boxes in MILP and its application. IET Inf. Secur. **13**(5), 479–485 (2019). https://doi.org/10.1049/IET-IFS.2018.5284
9. Liu, Y., Liang, H., Li, M., Huang, L., Hu, K., Yang, C., Wang, M.: STP models of optimal differential and linear trail for S-box based ciphers. Cryptology ePrint Archive, Report 2019/025 (2019), https://eprint.iacr.org/2019/025
10. Matsui, M.: On correlation between the order of S-boxes and the strength of DES. In: Santis, A.D. (ed.) EUROCRYPT'94. LNCS, vol. 950, pp. 366–375. Springer, Berlin, Heidelberg (May 1995). https://doi.org/10.1007/BFb0053451

11. MeiLing, Z., JingMei, L., XinMei, W.: The upper bounds on differntial characteristics in block cipher SMS4. Cryptology ePrint Archive, Report 2010/155 (2010), https://eprint.iacr.org/2010/155
12. Mouha, N., Preneel, B.: A proof that the ARX cipher Salsa20 is secure against differential cryptanalysis. IACR Cryptol. ePrint Arch. p. 328 (2013)
13. Mouha, N., Wang, Q., Gu, D., Preneel, B.: Differential and linear cryptanalysis using mixed-integer linear programming. In: Wu, C., Yung, M., Lin, D. (eds.) Information Security and Cryptology - 7th International Conference, Inscrypt 2011, Beijing, China, November 30 - December 3, 2011. Revised Selected Papers. Lecture Notes in Computer Science, vol. 7537, pp. 57–76. Springer (2011). https://doi.org/10.1007/978-3-642-34704-7_5
14. Sinz, C.: Towards an optimal CNF encoding of boolean cardinality constraints. In: van Beek, P. (ed.) Principles and Practice of Constraint Programming - CP 2005, 11th International Conference, CP 2005, Sitges, Spain, October 1-5, 2005, Proceedings. Lecture Notes in Computer Science, vol. 3709, pp. 827–831. Springer (2005). https://doi.org/10.1007/11564751_73
15. Su, B., Wu, W., Zhang, W.: Differential cryptanalysis of SMS4 block cipher. Cryptology ePrint Archive, Report 2010/062 (2010), https://eprint.iacr.org/2010/062
16. Sun, L., Wang, M.: Sok: Modeling for large S-boxes oriented to differential probabilities and linear correlations. IACR Trans. Symmetric Cryptol. **2023**(1), 111–151 (2023). https://doi.org/10.46586/TOSC.V2023.I1.111-151
17. Sun, L., Wang, W., Wang, M.: Accelerating the search of differential and linear characteristics with the SAT method. IACR Trans. Symm. Cryptol. **2021**(1), 269–315 (2021). https://doi.org/10.46586/tosc.v2021.i1.269-315
18. Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X., Song, L.: Automatic security evaluation and (related-key) differential characteristic search: Application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014, Part I. LNCS, vol. 8873, pp. 158–178. Springer, Berlin, Heidelberg (Dec 2014). https://doi.org/10.1007/978-3-662-45611-8_9
19. Wang, S., Feng, D., Hu, B., Guan, J., Zhang, K., Shi, T.: New method for combining Matsui's bounding conditions with sequential encoding method. DCC **91**(11), 3603–3642 (2023). https://doi.org/10.1007/s10623-023-01259-9
20. Wu, S., Wang, M.: Security evaluation against differential cryptanalysis for block cipher structures. Cryptology ePrint Archive, Report 2011/551 (2011), https://eprint.iacr.org/2011/551
21. Zhang, J., Wu, W., Zheng, Y.: Security of SM4 against (related-key) differential cryptanalysis. In: Bao, F., Chen, L., Deng, R.H., Wang, G. (eds.) Information Security Practice and Experience - 12th International Conference, ISPEC 2016, Zhangjiajie, China, November 16-18, 2016, Proceedings. Lecture Notes in Computer Science, vol. 10060, pp. 65–78 (2016). https://doi.org/10.1007/978-3-319-49151-6_5