Distinguisher and Related-Key Attack on HALFLOOP-96

Jinpeng Liu[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. HALFLOOP-96 is a 96-bit tweakable block cipher used in high frequency radio to secure automatic link establishment messages. In this paper, we concentrate on its differential properties in the contexts of conventional, related-tweak, and related-key differential attacks. Using automatic techniques, we determine the minimum number of active S-boxes and the maximum differential probability in each of the three configurations. The resistance of HALFLOOP-96 to differential attacks in the conventional and related-tweak configurations is good, and the longest distinguishers in both configurations consist of five rounds. In contrast, the security of the cipher against differential attacks in the related-key configuration is inadequate. The most effective related-key distinguisher we can find spans eight rounds. The 8-round related-key differential distinguisher is then utilised to initiate a 9-round weak-key attack. With $2^{92.96}$ chosen-plaintexts, 38.77-bit equivalent information about the keys can be recovered. Even though the attack does not pose a significant security threat to HALFLOOP-96, its security margin in the related-key configuration is exceedingly narrow. Therefore, improper use must be avoided in the application.

Keywords: Differential cryptanalysis · Related-tweak · Related-key · HALFLOOP-96.

1 Introduction

HALFLOOP is a family of tweakable block ciphers. It was created to encrypt protocol data units before transmission during automatic link establishment (ALE). HALFLOOP has been standardised in the most recent revision of MIL-STD-188-141D [1], the interoperability and performance standards for medium and high frequency radio systems issued by the United States Department of Defence.

The three versions of HALFLOOP, namely HALFLOOP-24, HALFLOOP-48, and HALFLOOP-96, possess the same key size of 128 bits while exhibiting differing state sizes of 24 bits, 48 bits, and 96 bits, correspondingly. The three variants of HALFLOOP are used in various generations of ALE systems: HALFLOOP-24 in the second generation (2G) system, HALFLOOP-48 in the third generation (3G) system, and HALFLOOP-96 in the fourth generation (4G) system.

The announcement of HALFLOOP is not accompanied by a public cryptanalysis. Dansarie *et al.* [12] presented the first public cryptanalytic result on HALFLOOP-24 and proposed a number of differential attacks [5] for ciphertext-only, known-plaintext, chosen-plaintext, and chosen-ciphertext scenarios. Despite having a 128-bit key size, the results of the attack indicate that HALFLOOP-24 is incapable of providing 128-bit security. Note that [12] only assesses the security of HALFLOOP-24 and does not examine the security of the other two variants.

Despite the fact that many HALFLOOP operations are derived from AES [2], HALFLOOP-96 is the most similar to AES of the three HALFLOOP variants. It is common knowledge that AES is susceptible to relate-key differential attacks, and full-round attacks on AES-192 and AES-256 are proposed in [6,7]. Consequently, the similarity between AES and HALFLOOP-96 drives us to investigate the security of HALFLOOP-96 in the context of related-key differential attacks.

1.1 Our Results

Motivated by recognising the resistance of HALFLOOP-96 to differential attack in the relate-key setting, we examine its differential property in the contexts of conventional, related-tweak, and related-key differential attacks. Automatic methods based on the Boolean satisfiability problem (SAT) are employed to find the lower bound on the number of active S-boxes and the upper bound on the differential probability for each of the three configurations.

- ❖ The resistance of HALFLOOP-96 to standard differential attacks is acceptable. The longest distinguisher with a probability above 2^{-95} covers five rounds. The probability of the optimal 5-round differential characteristic is 2^{-92}, whereas the accumulated probability of the best 5-round differential we can discover is $2^{-89.18}$. Due to the limited accumulated effect of differential characteristics, there is no effective 6-round distinguisher.
- ❖ Comparing the security of HALFLOOP-96 in the related-tweak setting to the security of the cipher in the conventional differential setting, there is no significant decline. The bounds on the active S-boxes and differential probability in the related-tweak setting are identical to those in the conventional setting, commencing from the sixth round. For more than five rounds, the differential characteristics returned by the SAT solver are the same as those with zero tweak differences. Therefore, starting with the sixth round, the performance of related-tweak differential characteristics is not superior to that of traditional differential characteristics.
- ❖ In the related-key setting, HALFLOOP-96 has a low resistance to differential attack. The maximum number of rounds covered by a related-key differential characteristic is eight. The probability of the unique 8-round related-key differential characteristic is 2^{-124}, whereas the probability of the key schedule

is 2^{-34} and the probability of the round function is 2^{-90}. The security margin in this case is limited, considering the ten rounds of HALFLOOP-96.

Using the newly discovered 8-round related-key differential distinguisher, we launch a 9-round related-key differential attack to recover partial information about the key pair. It takes $2^{92.96}$ chosen-plaintexts and $2^{92.96}$ 9-round encryptions to retrieve 38.77 bits of equivalent key information. The attack has a 90% success probability and is effective against 2^{94} key pairs with a specified difference. Although the attack does not pose an actual security threat to HALFLOOP-96, the security margin of the cipher in the setting for related-key attack is reduced to only one round. Hence, it is crucial to take measures to avoid the improper use of the application.

Outline. Section 2 goes over the target cipher HALFLOOP-96 as well as differential cryptanalysis. Section 3 describes the procedure for developing SAT models to seek for differential distinguishers of HALFLOOP-96. Section 4 provides the differential properties of the cipher in the conventional, related-tweak, and related-key configurations. The 9-round related-key differential on HALFLOOP-96 is detailed in Section 5. Section 6 serves as the conclusion of the paper.

2 Preliminaries

In this section, the cipher examined in the paper is initially reviewed. Next, the primary concept of differential cryptanalysis is presented.

2.1 Description of HALFLOOP-96

HALFLOOP [1] is a tweakable block cipher family with three distinct variants. HALFLOOP-96 employs 96-bit blocks and has 128-bit key K and 64-bit tweak T. Many operations in HALFLOOP-96 are derived from AES [2].

Initialisation After receiving the plaintext $m = m_0 \| m_1 \| \cdots \| m_{11}$, where $m_i \in \mathbb{F}_2^8$, $0 \leqslant i \leqslant 11$, the internal state $\mathtt{IS}$ is created by setting $\mathtt{IS}$ as

$$\mathtt{IS} = \begin{bmatrix} m_0 & m_4 & m_8 \\ m_1 & m_5 & m_9 \\ m_2 & m_6 & m_{10} \\ m_3 & m_7 & m_{11} \end{bmatrix}.$$

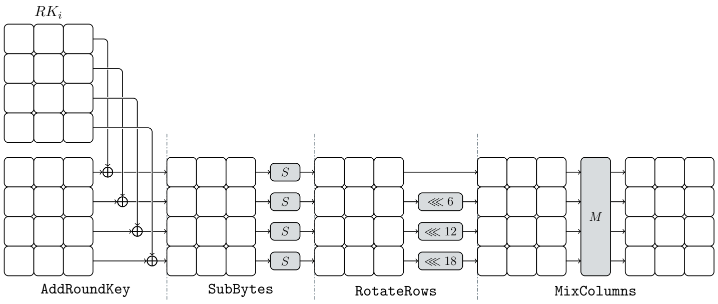


Fig. 1. Round function of HALFLOOP-96.

A single encryption round consists of the four operations depicted in Fig. 1: `AddRoundKey` (`ARK`), `SubBytes` (`SB`), `RotateRows` (`RR`), and `MixColumns` (`MC`). The encryption process consists of $r = 10$ rounds, with the last round replacing the `MixColumns` operation with `AddRoundKey`. The definitions of the four operations are as follows.

`AddRoundKey` (`ARK`) The round key RK_i is bitwise added to the state in the i-th round.

`SubBytes` (`SB`) An 8-bit S-box S is applied to each byte of the state, which is identical to the S-box used by AES (cf. [2]).

`RotateRows` (`RR`) As shown in Fig. 1, this operation rotates the rows of the state to the left by a variable number of bit positions.

`MixColumns` (`MC`) This operation is the same as the MixColumn transformation used in AES. The columns of the state are regarded as polynomials over the finite field $\mathbb{F}_{2^8}$, with the irreducible binary polynomial denoted as $m(x) = x^8 + x^4 + x^3 + x + 1$. Each column is multiplied modulo $x^4 + 1$ by a fixed polynomial $c(x)$ given by $c(x) = 3 \cdot x^3 + x^2 + x + 2$. The aforementioned process can instead be represented as a matrix multiplication utilising the matrix M over $\mathbb{F}_{2^8}$. In this case, the matrix M is defined as

$$M = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}. \qquad (1)$$

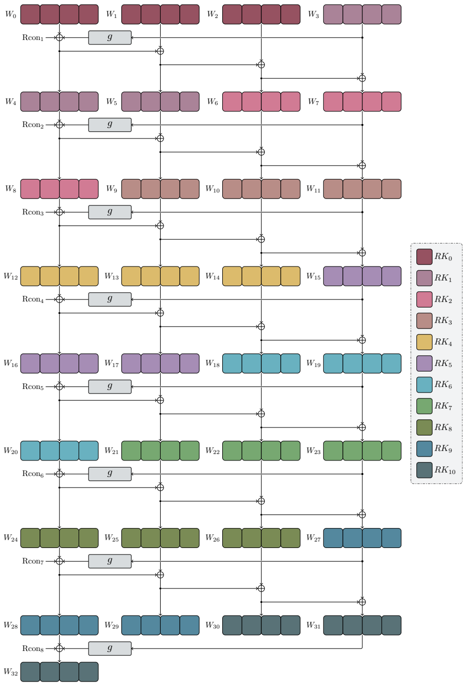


Fig. 2. Key schedule of HALFLOOP-96.

Key Schedule The key schedule resembles that of AES-128 closely. Denote K and T as $K_0\|K_1\|K_2\|K_3$ and $T_0\|T_1$, respectively, where K_i $(0 \leqslant i \leqslant 3)$ and T_j $(j = 0, 1)$ are 32-bit words. K and T are utilised to generate a linear array of 4-byte words W_0, W_1, …, W_{32}, which are then employed to create the round keys. The first four words are initialised with

$$W_0 = K_0 \oplus T_0, W_1 = K_1 \oplus T_1, W_2 = K_2, W_3 = K_3.$$

The remaining words are derived using the subsequent two functions.

`RotWord` The function accepts the input word $a_0\|a_1\|a_2\|a_3$, performs a cyclic permutation, and returns the output word $a_1\|a_2\|a_3\|a_0$.

`SubWord` The function takes a 4-byte input word and applies the S-box S to each of the four bytes to generate a 4-byte output word.

Each subsequent word W_i $(4 \leqslant i \leqslant 32$ and $i \bmod 4 \neq 0)$ is the XOR of the two preceding words W_{i-1} and W_{i-4}. For words in positions i that are a multiple of four, $g = \texttt{SubWord} \circ \texttt{RotWord}$ is applied to W_{i-1} prior to the XOR, and a round constant $\mathrm{Rcon}_{i/4}$ is XORed with the result. Eight round constants are involved in the key schedule of HALFLOOP-96, which are

$$\mathrm{Rcon}_1 = \texttt{0x01000000}, \mathrm{Rcon}_2 = \texttt{0x02000000}, \mathrm{Rcon}_3 = \texttt{0x04000000},$$
$$\mathrm{Rcon}_4 = \texttt{0x08000000}, \mathrm{Rcon}_5 = \texttt{0x10000000}, \mathrm{Rcon}_6 = \texttt{0x20000000},$$
$$\mathrm{Rcon}_7 = \texttt{0x40000000}, \mathrm{Rcon}_8 = \texttt{0x80000000}.$$

To obtain the round keys RK_0, RK_1, …, and RK_{10} for HALFLOOP-96, it is necessary to repackage the 4-byte words into 12-byte words. The key schedule is illustrated in Fig. 2.

2.2 Differential Cryptanalysis

The concept of differential cryptanalysis was initially introduced by Biham and Shamir [5] at CRYPTO 1990. The fundamental methodology involves using plaintext pairs (P, P') linked by a constant *input difference* Δ_{in}, commonly described as the XOR operation between two plaintexts. The attacker subsequently calculates the difference between the two ciphertexts (C, C') to identify a non-random occurrence of an *output difference* Δ_{out} with a certain likelihood.

The pair of differences $(\Delta_{\mathsf{in}}, \Delta_{\mathsf{out}})$ is called a *differential*. The differential probability of the differential over an n-bit primitive E_K is computed as

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

The *weight* of the differential is determined by taking the negative logarithm of its probability, using a base of two.

The task of evaluating the differential probability of a differential in order to discover a valid differential for a cryptographic algorithm with several iterations is known to be quite challenging. The differential is usually localised by constructing *differential characteristics*, which enable the tracking of differences occurring after each round. Let $(\Delta_0 = \Delta_{\mathsf{in}}, \Delta_1, \ldots, \Delta_r = \Delta_{\mathsf{out}})$ be an r-round differential characteristic of the given differential $(\Delta_{\mathsf{in}}, \Delta_{\mathsf{out}})$. Suppose the r-round encryption E_K can be represented as the composition of r round functions denoted by $f_{k_{r-1}} \circ f_{k_{r-2}} \circ \cdots \circ f_{k_0}$. Given the premise that the round keys k_0, k_1, …, and k_{r-1} are independent and uniformly random, the differential probability of the differential characteristic can be calculated as

$$\mathrm{Pr}_{E_K}(\Delta_0, \Delta_1, \ldots, \Delta_r) = \prod_{i=0}^{r-1} \mathrm{Pr}_{f_{k_i}}(\Delta_i, \Delta_{i+1}).$$

As discussed in [14], a fixed differential might encompass several differential characteristics, and the probability of the differential is determined by aggregating the probabilities associated with each differential characteristic. This probability may be computed as

$$\mathrm{Pr}_{E_K}(\Delta_{\mathsf{in}}, \Delta_{\mathsf{out}}) = \sum_{\Delta_1, \Delta_2, \ldots, \Delta_{r-1} \in \mathbb{F}_2^n} \mathrm{Pr}_{E_K}(\Delta_{\mathsf{in}}, \Delta_1, \ldots, \Delta_{r-1}, \Delta_{\mathsf{out}}).$$

In practical applications, the comprehensive search for all characteristics inside a differential and the precise calculation of their probabilities are unattainable due to the constraints imposed by limited computational resources. A common way of handling this is to find the differential characteristics with a higher probability in the differential, and the summation of probabilities of these characteristics approximates the probability of the differential.

After finding an r-round differential $(\Delta_{\mathsf{in}}, \Delta_{\mathsf{out}})$ with probability p_0 ($p_0 > 2^{1-n}$), we can launch an attack against the $(r+1)$-round encryption $\widehat{E}_K = f_{k_r} \circ E_K$. The following is a summary of the attack procedure.

① Select N pairs of plaintexts (P, P') whose difference $P \oplus P'$ equals Δ_{in}. Query the encryption oracle to obtain pairs of corresponding ciphertexts (C, C').

② Create a counter $\mathsf{Ctr}[k_r^{(i)}]$ for each possible value $k_r^{(i)}$ of the subkey k_r, $0 \leqslant i \leqslant 2^n - 1$. For each pair (C, C'), determine the value of $f^{-1}_{k_r^{(i)}}(C) \oplus f^{-1}_{k_r^{(i)}}(C')$ for each $k_r^{(i)}$. If the equation $f^{-1}_{k_r^{(i)}}(C) \oplus f^{-1}_{k_r^{(i)}}(C') = \Delta_{\mathsf{out}}$ is valid, increment the counter $\mathsf{Ctr}[k_r^{(i)}]$ by one.

③ If the threshold is set to τ, the key guess $k_r^{(i)}$ is sorted into a candidate list only if the counter value $\mathsf{Ctr}[k_r^{(i)}]$ is at least τ.

The counter that keeps track of the number of pairs confirming the differential conforms to the binomial distribution $\mathcal{B}(N, p_0)$ when the correct key guess is made, as the attack procedure specifies. The counter under the wrong key guess follows a binomial distribution $\mathcal{B}(N, p)$, where p is the probability of a pair matching the differential given a wrong key guess, which is equal to $p = 2^{1-n}$.

As a statistical cryptanalysis, differential cryptanalysis is inevitably confronted with two errors. The symbol ε_0 denotes the likelihood that the candidate list does not include the right key. The likelihood of a key guess that is not correct remaining in the candidate list is represented by the symbol ε_1. Hence, the probability of success (P_S) in the attack, denoting the likelihood of the right key being included in the candidate list, may be expressed as $1 - \varepsilon_0$. When the value of N is sufficiently large, the approximations for ε_0 and ε_1 may be derived using the methodology presented in [8] as

$$\begin{aligned} \varepsilon_0 &\approx \frac{p_0 \cdot \sqrt{1 - (\tau - 1)/N}}{(p_0 - (\tau - 1)/N) \cdot \sqrt{2 \cdot \pi \cdot (\tau - 1)}} \cdot \exp\left[-N \cdot D\left(\frac{\tau - 1}{N} \middle\| p_0\right)\right], \\ \varepsilon_1 &\approx \frac{(1 - p) \cdot \sqrt{\tau/N}}{(\tau/N - p) \cdot \sqrt{2 \cdot \pi \cdot N \cdot (1 - \tau/N)}} \cdot \exp\left[-N \cdot D\left(\frac{\tau}{N} \middle\| p\right)\right], \end{aligned} \tag{2}$$

where $D(p\|q) \triangleq p \cdot \ln\left(\frac{p}{q}\right) + (1 - p) \cdot \ln\left(\frac{1-p}{1-q}\right)$ represents the Kullback-Leibler divergence between two Bernoulli distributions with parameters p and q.

2.3 Related-Key and Related-Tweak Differential Cryptanalysis

One notable distinction between differential cryptanalysis and related-key differential cryptanalysis is the utilisation of differential propagations. In related-key differential cryptanalysis, the focus is on exploiting the differential propagation while encrypting plaintexts P and P' with distinct keys, even if these plaintexts happen to be identical. The formal representation of an r-round *related-key differential* is denoted by the triple $(\Delta_{\mathsf{in}}, \Delta_{\mathsf{out}}, \Delta_{\mathsf{key}})$, where Δ_{key} signifies the difference between the keys. The probability is calculated as

$$\mathrm{Pr}_{E_K}(\Delta_{\mathsf{in}}, \Delta_{\mathsf{out}}, \Delta_{\mathsf{key}}) = \frac{\{x \in \mathbb{F}_2^n \mid E_K(x) \oplus E_{K \oplus \Delta_{\mathsf{key}}}(x \oplus \Delta_{\mathsf{in}}) = \Delta_{\mathsf{out}}\}}{2^n}.$$

AES is widely acknowledged as vulnerable to related-key differential attacks, as evidenced by the suggested full-round attacks on AES-192 and AES-256 in [6,7]. Given that HALFLOOP-96 has the highest degree of similarity to AES among the three HALFLOOP variations, our focus lies on examining its differential property in the context of a related-key attack.

It is also feasible to initialise related-tweak differential cryptanalysis for tweakable block ciphers. Differential propagation is utilised when P and P', which might potentially be identical, are encrypted using the same key and distinct tweaks. The *related-tweak differential* is denoted by $(\Delta_{\mathsf{in}}, \Delta_{\mathsf{out}}, \Delta_{\mathsf{tweak}})$, where Δ_{tweak} signifies the difference between the tweaks. In contrast to related-key differential cryptanalysis, related-tweak differential cryptanalysis is considered a more feasible approach because the adversary knows the value of the tweak.

3 Automatic Search of Differential Distinguishers

Identifying a differential with a non-negligible probability is a pivotal and arduous stage in a differential attack. At the EUROCRYPT 1994, Matsui [18] introduced a pioneering approach called the branch and bound algorithm, which offered a systematic methodology for investigating the best differential characteristic. When considering tailored optimisations for certain ciphers, it is indisputable that branch and bound algorithms exhibit high efficiency [13]. However, the ability to prevent memory overflow through the precise selection of search nodes is a challenge requiring proficiency in cryptanalysis and programming.

The introduction of automatic search techniques [19] has dramatically simplified the process of identifying differential characteristics. The main aim is to transform the task of finding differential characteristics into some well-studied mathematical problems. With some publicly accessible solvers for these mathematical problems, the optimal differential characteristics can be identified. Due to its relatively straightforward implementation, automatic approaches have been widely employed in the search for distinguishers in various attacks.

The mathematical problems that are commonly encountered include mixed integer linear programming (MILP), Boolean satisfiability problem (SAT), satisfiability modulus theories (SMT), and constraint satisfaction problem (CSP). The classification of automatic search methods is based on the mathematical issues they address. The search for differential characteristics in ciphers with 8-bit S-boxes may be conducted using MILP method as described in [3,9,15], SAT method as described in [4,23], and SMT method as described in [16]. In this study, the SAT method proposed in [23] is chosen for efficiently generating SAT models for S-boxes.

This section provides a comprehensive description of the SAT models necessary for searching for differential characteristics of HALFLOOP-96.

3.1 Boolean Satisfiability Problem

A *Boolean formula* is comprised of Boolean variables, the operations AND (conjunction, $\wedge$), OR (disjunction, $\vee$), and NOT (negation, $\bar{\cdot}$), and brackets. The *Boolean satisfiability problem* (SAT) pertains to ascertaining the existence of a valid assignment for all Boolean variables such that the given Boolean formula holds. If this condition is met, the formula is known as *satisfiable*. In the absence of such a designated task, the formula in question is considered *unsatisfiable*. SAT is the first problem proven to be NP-complete [11]. However, significant advancements have been made in developing efficient solvers capable of handling a substantial volume of real-world SAT problems.

This work employs the solver CryptoMiniSat [21] for distinguisher search. CryptoMiniSat necessitates that Boolean formulae be expressed in *conjunctive normal form* (CNF), whereby many *clauses* are made in conjunction with each other, and each clause consists of a disjunction of variables, which may be negated. CryptoMiniSat additionally provides support for *XOR clauses* that are formed of XOR operations on variables. This feature greatly simplifies the process of constructing models for HALFLOOP-96. Converting distinguisher searching problems into Boolean formulae is critical in developing automatic models.

3.2 SAT Models for Linear Operations of HALFLOOP-96

For the m-bit vector Δ, the i-th bit ($0 \leqslant i \leqslant m-1$) is denoted by $\Delta[i]$, while $\Delta[0]$ represents the most significant bit.

Model 1 (XOR, [17]) *For the m-bit XOR operation, the input differences are represented by Δ_0 and Δ_1, and the output difference is denoted by Δ_2. Differential propagation is valid if and only if the values of Δ_0, Δ_1 and Δ_2 validate all of the following XOR clauses.*

$$\Delta_0[i] \oplus \Delta_1[i] \oplus \Delta_2[i] = 0, 0 \leqslant i \leqslant m-1.$$

To build the model for the `MC` operation, we employ the procedure described in [24]. First, the *primitive representation* [22] $\mathbb{M}$ of the matrix M (cf. Eqn. (1))

is created.

$$\mathbb{M} = \left[\begin{array}{cccccccc:cccccccc:cccccccc:cccccccc}
0&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0\\
1&0&0&0&1&0&0&0&1&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0\\
1&0&0&0&0&1&0&0&1&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0\\
1&0&0&0&0&0&0&1&1&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0\\
1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1\\
\hdashline
1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&0&0&1&0&0&0&0&1&0&0&1&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&1&1&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1\\
\hdashline
1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&1&1&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&1&0&0&1&0&0&0&1&1&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&1&1&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1\\
\hdashline
1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0\\
1&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&0\\
1&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&1&0&0\\
0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0\\
1&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&1\\
1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0
\end{array}\right]$$

is the matrix representation of M over $\mathbb{F}_2$. The notation $\mathbb{M}_{i,j}$ represents the element located in the i-th row and j-th column of the matrix $\mathbb{M}$. The SAT model can then be constructed using XOR clauses.

Model 2 (Matrix Multiplication) *For matrix multiplication with the 32×32 matrix $\mathbb{M}$, the input and output differences are represented by Δ_0 and Δ_1 respectively. Differential propagation is valid if and only if the values of Δ_0 and Δ_1 satisfy all the XOR clauses in the subsequent.*

$$\bigoplus_{\{j \mid 0 \leqslant j \leqslant 31 \ s.t. \ \mathbb{M}_{i,j}=1\}} \Delta_0[j] \oplus \Delta_1[i] = 0, 0 \leqslant i \leqslant 31.$$

3.3 SAT Model for the S-box of HALFLOOP-48

The method in [23] is utilised to construct the SAT model for the S-box. We commence our analysis with the SAT model that is focused on active S-boxes. In addition to using 16 Boolean variables $\Delta_0 = (\Delta_0[0], \Delta_0[1], \ldots, \Delta_0[7])$ and

$\Delta_1 = (\Delta_1[0], \Delta_1[1], \ldots, \Delta_1[7])$ to represent the input and output differences of the S-box, it is necessary to incorporate an auxiliary Boolean variable denoted as w. The value assigned to w is one for active S-boxes and zero for inactive S-boxes, assuming the propagation $\Delta_0 \to \Delta_1$ is possible. Based on the given criteria, the set

$$\mathcal{V}_1 = \left\{ \Delta_0 \| \Delta_1 \| w \;\middle|\; \begin{array}{l} \Delta_0, \Delta_1 \in \mathbb{F}_2^8, w \in \mathbb{F}_2 \\ w = \begin{cases} 1, & \text{if } \Pr_S(\Delta_0, \Delta_1) < 1 \\ 0, & \text{if } \Pr_S(\Delta_0, \Delta_1) = 1 \end{cases} \end{array} \right\}$$

encompasses potential values for $\Delta_0 \| \Delta_1 \| w$. In order to maintain the constraint that $\Delta_0 \| \Delta_1 \| w$ remains within the bounds of the set $\mathcal{V}_1$, a clause is generated for each 17-bit vector $v \notin \mathcal{V}_1$,

$$\bigvee_{i=0}^{7} (\Delta_0[i] \oplus v[i]) \vee \bigvee_{i=0}^{7} (\Delta_1[i] \oplus v[i+8]) \vee (w \oplus v[16]) = 1,$$

which may serve as a candidate for the SAT model of the S-box. These clauses comprise an initial version of the SAT model for the search oriented to active S-boxes. The use of the initial version of the SAT model without modification would impede the search process of the automatic method due to the large size of the set $\mathbb{F}_2^{17} \backslash \mathcal{V}_1$, which is $2^{17} - 32386 = 98686$. To reduce the size of the S-box model, we employ the Espresso algorithm [10] to simplify the model[4]. The final SAT model oriented to active S-boxes is composed of 7967 clauses.

The SAT model oriented to differential probability can be created similarly. The probabilities of possible differential propagations $\Delta_0 \to \Delta_1$ for the 8-bit S-box S can take values from the set $\{2^{-7}, 2^{-6}, 1\}$. Motivated by the two-step encoding method described in [23], we introduce two Boolean variables u_0 and u_1 for each S-box to encode the differential probability of possible propagations.

$$\mathcal{V}_2 = \left\{ \Delta_0 \| \Delta_1 \| u_0 \| u_1 \;\middle|\; \begin{array}{l} \Delta_0, \Delta_1 \in \mathbb{F}_2^8, u_0, u_1 \in \mathbb{F}_2 \\ u_0 \| u_1 = \begin{cases} 1\|1, & \text{if } \Pr_S(\Delta_0, \Delta_1) = 2^{-7} \\ 0\|1, & \text{if } \Pr_S(\Delta_0, \Delta_1) = 2^{-6} \\ 0\|0, & \text{if } \Pr_S(\Delta_0, \Delta_1) = 1 \end{cases} \end{array} \right\}$$

is an optional set of values that may be assigned to the vector $\Delta_0 \| \Delta_1 \| u_0 \| u_1$. Thus, the weight of a potential propagation can be determined by $u_0 + 6 \cdot u_1$. To ensure that $\Delta_0 \| \Delta_1 \| u_0 \| u_1$ never takes values outside of the set $\mathcal{V}_2$, we should generate a clause for each 18-bit $\nu \notin \mathcal{V}_2$,

$$\bigvee_{i=0}^{7} (\Delta_0[i] \oplus \nu[i]) \vee \bigvee_{i=0}^{7} (\Delta_1[i] \oplus \nu[i+8]) \vee (u_0 \oplus \nu[16]) \vee (u_1 \oplus \nu[17]) = 1.$$

[4] A modern, compilable re-host of the Espresso heuristic logic minimizer can be found at https://github.com/classabbyamp/espresso-logic.

These clauses constitute an initial version of the SAT model oriented to differential probability. ESPRESSO algorithm is once again employed to reduce the size of the model. The final S-box model oriented to differential probability is composed of 8728 clauses.

3.4 SAT Model for the Objective Function

We aim to identify differential characteristics that exhibit fewer active S-boxes and high probability. The objective function can be mathematically expressed as $\sum_{i=0}^{\ell} u_i \leqslant \vartheta$, where u_i $(0 \leqslant i \leqslant \ell)$ are Boolean variables that indicate the activation status of the S-boxes or encode the differential probability of possible propagations for the S-boxes. Let ϑ denote a predetermined upper limit for either the number of active S-boxes or the weight of the differential characteristics. The sequential encoding method [20] is utilised to transform this inequality into clauses.

Model 3 (Objective Function, [20]) *The following clauses provide validity assurance for the objective function* $\sum_{i=0}^{\ell} u_i \leqslant 0$.

$$\overline{u_i} = 1, 0 \leqslant i \leqslant \ell.$$

For the objective function $\sum_{i=0}^{\ell} u_i \leqslant \vartheta$ *with* $\vartheta > 0$*, it is necessary to incorporate auxiliary Boolean variables* $a_{i,j}$ $(0 \leqslant i \leqslant \ell - 1, 0 \leqslant j \leqslant \vartheta - 1)$*. The objective function is valid if and only if the following clauses hold.*

$$\begin{array}{l}
\overline{u_0} \vee a_{0,0} = 1\\
\overline{a_{0,j}} = 1,\ 1 \leqslant j \leqslant \vartheta - 1\\
\left.\begin{array}{l}
\overline{u_i} \vee a_{i,0} = 1\\
\overline{a_{i-1,0}} \vee a_{i,0} = 1\\
\left.\begin{array}{l}\overline{u_i} \vee \overline{a_{i-1,j-1}} \vee a_{i,j} = 1\\ \overline{a_{i-1,j}} \vee a_{i,j} = 1\end{array}\right\} 1 \leqslant j \leqslant \vartheta - 1\\
\overline{u_i} \vee \overline{a_{i-1,\vartheta-1}} = 1
\end{array}\right\} 1 \leqslant i \leqslant \ell - 2\\
\overline{u_\ell} \vee \overline{a_{\ell-1,\vartheta-1}} = 1
\end{array}.$$

3.5 Finding More Differential Characteristics

Using the models presented in Sections 3.2 to 3.4, we can identify differential characteristics with fewer active S-boxes and high probabilities. To improve the probability evaluation of the differential, we should fix the input and output differences in the automatic model and find as many other differential characteristics as feasible. To prevent the solver from returning the same solution after obtaining a single differential characteristic, we should add a clause to the SAT problem. Assume that $v \in \mathbb{F}_2^\omega$ is a solution for the ω Boolean variables x_0, x_1, $\ldots$, $x_{\omega-1}$ returned by the SAT solver. Two index sets

$$v|_0 = \{i|0 \leqslant i \leqslant \omega - 1 \text{ s.t. } v[i] = 0\}, \text{ and } v|_1 = \{i|0 \leqslant i \leqslant \omega - 1 \text{ s.t. } v[i] = 1\}.$$

are generated based on the value of v. Adding the clause

$$\bigvee_{i \in v|_0} x_i \vee \bigvee_{i \in v|_1} \overline{x_i} = 1$$

to the SAT problem guarantees that the solver will not find v again.

4 Differential Distinguishers of HALFLOOP-96

This section presents an analysis of the differential characteristics of HALFLOOP-96 in three attack settings: conventional, related-tweak, and related-key. These characteristics are determined using the methodology in Section 3.

Table 1. Differential properties of HALFLOOP-96.

Round	1	2	3	4	5	6	7	8	9	10
#S	1	5	8	11	14	17	20	23	26	29
$\#\mathtt{S}_\mathtt{T}$	0	1	3	8	14	17	20	23	26	29
$\#\mathtt{S}_\mathtt{K}$	0	0	1	5	11	14	16	19	24	29
P	2^{-6}	2^{-30}	2^{-48}	2^{-70}	2^{-92}	2^{-113}	2^{-134}	2^{-155}	2^{-176}	2^{-197}
$\mathtt{P}_\mathtt{T}$	1	2^{-6}	2^{-18}	2^{-53}	2^{-91}	2^{-113}	2^{-134}	2^{-155}	2^{-176}	2^{-197}
$\mathtt{P}_\mathtt{K}$	1	1	2^{-6}	2^{-31}	2^{-66}	2^{-87}	2^{-106}	2^{-124}	2^{-154}	2^{-197}

#S, $\#\mathtt{S}_\mathtt{T}$, and $\#\mathtt{S}_\mathtt{K}$: The number of active S-boxes in conventional, related-tweak, and related-key settings.

P, $\mathtt{P}_\mathtt{T}$, and $\mathtt{P}_\mathtt{K}$: Differential probabilities in conventional, related-tweak, and related-key settings.

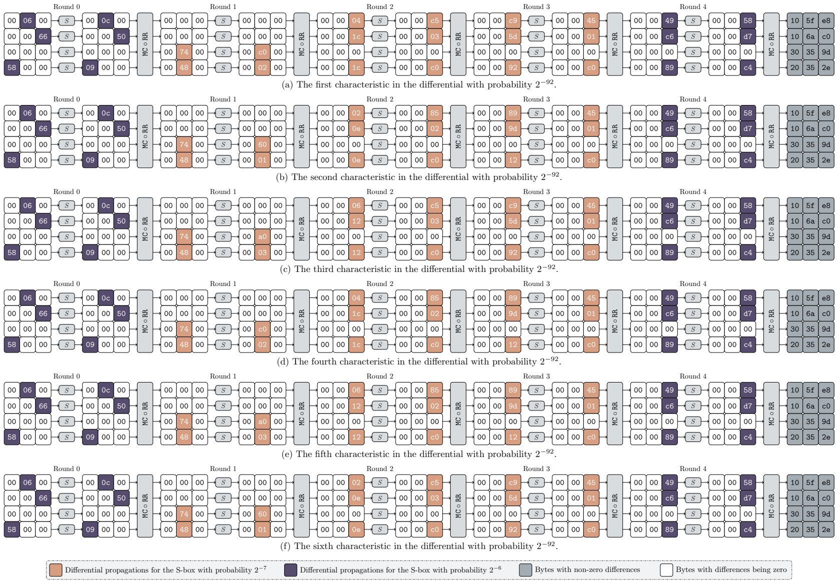
4.1 Conventional Differential Distinguishers of HALFLOOP-96

The lower bound on the number of active S-boxes and the upper bound on the differential probability are calculated in the standard differential attack scenario. The outcomes of 1 to 10 rounds of HALFLOOP-96 are displayed in Table 1.

Table 2. Information about three 5-round differentials with probability $2^{-89.18}$.

Index	Input difference	Output difference
1	0x000000580600000000660000	0x101030205f6a3535e8c09d2e
2	0x060000000066000000000058	0x5f6a3535e8c09d2e10103020
3	0x006600000000005806000000	0xe8c09d2e101030205f6a3535

The longest differential characteristic with a probability greater than 2^{-95} spans five rounds, and the SAT solver indicates that there are 3207 5-round differential characteristics with probability 2^{-92}. A thorough analysis reveals that the 3207 characteristics stem from 2214 distinct differentials. We search for all differential characteristics in the 2214 differentials with probabilities more significant than 2^{-110} by fixing the input and output differences in the automatic search. The largest accumulated probability of the differential is $2^{-89.18}$, and there are three differentials with the highest probability, whose input and output differences are shown in Table 2. Six 5-round characteristics exist in the first differential with the highest probability of 2^{-92}, as depicted in Fig. 3.


Round 0
Round 1
Round 2
Round 3
Round 4
S
MC ∘ RR
Differential propagations for the S-box with probability 2^{-7}
Differential propagations for the S-box with probability 2^{-6}
Bytes with non-zero differences
Bytes with differences being zero

(a) The first characteristic in the differential with probability 2^{-92}.

(b) The second characteristic in the differential with probability 2^{-92}.

(c) The third characteristic in the differential with probability 2^{-92}.

(d) The fourth characteristic in the differential with probability 2^{-92}.

(e) The fifth characteristic in the differential with probability 2^{-92}.

(f) The sixth characteristic in the differential with probability 2^{-92}.

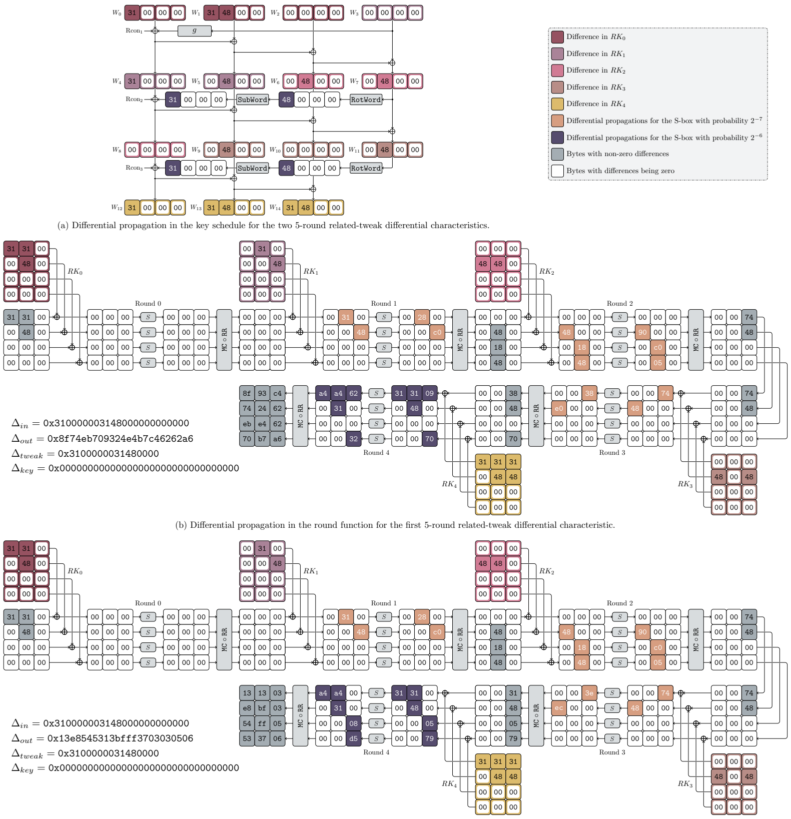
Fig. 3. Six dominated characteristics in the first 5-round differential.

Even though the probability of the optimal 6-round differential characteristic of HALFLOOP-96 is less than 2^{-95}, we question the existence of 6-round differentials with accumulated probabilities greater than 2^{-95}. To find the answer, we first search for all 6-round differential characteristics with a probability of 2^{-113} and determine that 1272 characteristics meet the condition. Note that the 1272 characteristics come from 1017 different differentials. Then, we fix the input and output differences in the automatic search and discover all differential characteristics with probabilities greater than 2^{-135} for each of the 1017 differentials. The maximal accumulated probability of 6-round differentials reaches $2^{-110.87}$, indicating that these differentials cannot support a valid differential attack. The longest differential distinguisher for HALFLOOP-96 comprises five rounds.

4.2 Related-Tweak Differential Distinguishers of HALFLOOP-96

The evaluation of active S-boxes and differential probabilities should include the key schedule in the context of a related-tweak attack. Table 1 displays the minimum number of active S-boxes and maximum differential probabilities for one to ten rounds of HALFLOOP-96 in the related-tweak attack configuration.

From the sixth round, the bounds on the active S-boxes and probabilities in the related-tweak setting are identical to those in the conventional setting, as shown in Table 1. The differential characteristics returned by the SAT solver for more than five rounds do not have non-zero tweak differences. Accordingly, beginning with the sixth round, related-tweak differential characteristics do not perform better than conventional ones. Given that the optimal differential in the conventional differential attack setting has already reached five rounds, the advantage of the adversary in the related-tweak setting is insignificant.


W_0 W_1 W_2 W_3
Rcon$_1$
g
W_4 W_5 W_6 W_7
Rcon$_2$
SubWord
RotWord
W_8 W_9 W_{10} W_{11}
Rcon$_3$
W_{12} W_{13} W_{14}
Difference in RK_0
Difference in RK_1
Difference in RK_2
Difference in RK_3
Difference in RK_4
Differential propagations for the S-box with probability 2^{-7}
Differential propagations for the S-box with probability 2^{-6}
Bytes with non-zero differences
Bytes with differences being zero
RK_0
RK_1
RK_2
RK_3
RK_4
Round 0
Round 1
Round 2
Round 3
Round 4
S
MC ∘ RR
Δ_{in} = 0x31000000314800000000000
Δ_{out} = 0x8f74eb709324e4b7c46262a6
Δ_{tweak} = 0x3100000031480000
Δ_{key} = 0x00000000000000000000000000000000
Δ_{in} = 0x31000000314800000000000
Δ_{out} = 0x13e8545313bfff3703030506
Δ_{tweak} = 0x3100000031480000
Δ_{key} = 0x00000000000000000000000000000000

(a) Differential propagation in the key schedule for the two 5-round related-tweak differential characteristics.

(b) Differential propagation in the round function for the first 5-round related-tweak differential characteristic.

(c) Differential propagation in the round function for the second 5-round related-tweak differential characteristic.

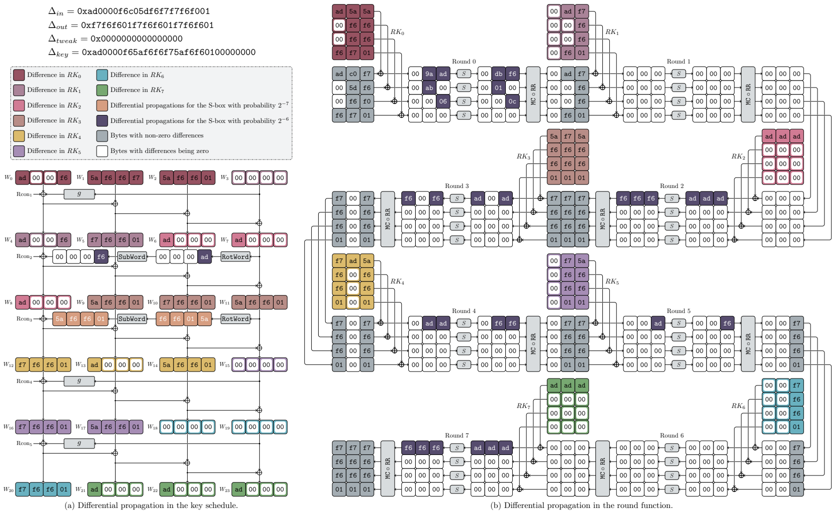
Fig. 4. Two 5-round related-tweak differential characteristics with probability 2^{-91}.

The minor advantage resides in the existence of 5-round related-tweak differential characteristics with a probability of 2^{-91}, whereas the probability of the optimal 5-round characteristic in the conventional setting is 2^{-92}. We find two 5-round related-tweak differential characteristics with a probability of 2^{-91} using the SAT solver. The probability in the key schedule is 2^{-12} and the probability in the round function is 2^{-79} for both characteristics. In addition, after searching exhaustively with the automatic procedure for all characteristics with probabilities greater than 2^{-120}, we are unable to identify a clustering effect for the two characteristics. Figure 4 exhibits the two characteristics.

4.3 Related-Key Differential Distinguishers of HALFLOOP-96

In the context of a related-key attack, the calculation of active S-boxes and differential probabilities must consider the key schedule. Table 1 displays the bounds on the active S-boxes and differential probabilities from one to ten cycles of HALFLOOP-96.

Note that in the related-key attack configuration, the characteristics may be utilised in an attack if the probability is greater than 2^{-127}. According to Table 1, the effective related-key differential characteristic with the most rounds is eight. We verify using the SAT solver that there is only one 8-round related-key differential characteristic with probability 2^{-124}. Figure 5 illustrates the 8-round characteristic. The probability in the key schedule is 2^{-34}, and the probability in the round function is 2^{-90}. In addition, we do not identify the clustering effect for the 8-round distinguisher after exhaustively searching for all characteristics with probability no less than 2^{-150}.



Δ_{in} = 0xad0000f6c05df6f7f7f6f001
Δ_{out} = 0xf7f6f601f7f6f601f7f6f601
Δ_{tweak} = 0x0000000000000000
Δ_{key} = 0xad0000f65af6f6f75af6f60100000000
Difference in RK_0
Difference in RK_1
Difference in RK_2
Difference in RK_3
Difference in RK_4
Difference in RK_5
Difference in RK_6
Difference in RK_7
Differential propagations for the S-box with probability 2^{-7}
Differential propagations for the S-box with probability 2^{-6}
Bytes with non-zero differences
Bytes with differences being zero
W_0 W_1 W_2 W_3 W_4 W_5 W_6 W_7
Rcon₁ g
Rcon₂ SubWord RotWord
Round 0 Round 1 Round 2 Round 3 Round 4 Round 5 Round 6 Round 7
RK_0 RK_1 RK_2 RK_3 RK_4 RK_5 RK_6 RK_7
S
MC∘RR

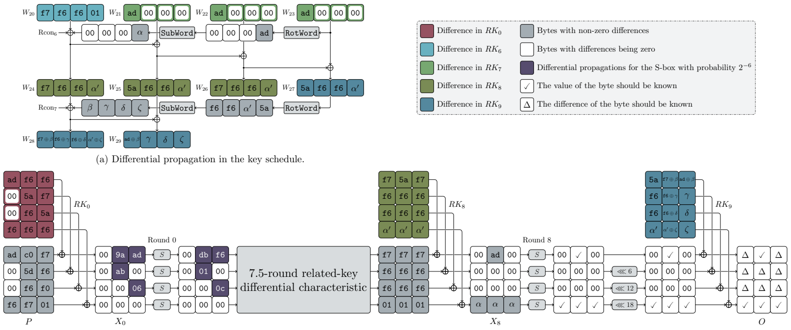
(a) Differential propagation in the key schedule.
(b) Differential propagation in the round function.

Fig. 5. 8-round related-key differential characteristics with probability 2^{-124}.

5 Related-Key Differential Attack on HALFLOOP-96

In this section, we employ the 8-round related-key differential distinguisher in Section 4.3 to launch a 9-round related-key differential attack on HALFLOOP-96. Note that the attack is a weak-key attack, as the probability of the key schedule shown in Fig. 5 is 2^{-34}. In other words, only one pair of keys out of 2^{34} pairs of keys with a difference of Δ_{key} = `0xad0000f65af6f6f75af6f60100000000` is susceptible to the following attack. In this circumstance, a valid attack must ensure the time complexity is less than 2^{94}.

In the attack, one round is appended after the distinguisher, and the key-recovery procedure is depicted in Fig. 6. $\mathcal{S}$ structures are prepared for the attack. Each structure contains 2^{80} plaintexts, where ten bytes $P[0, 3\text{-}11]$ of the plaintext P traverse all possible values while the remaining two are fixed to random constants. Then, a single structure can be used to create 2^{79} pairs with a difference of ΔP = `0xad0000f6c05df6f7f7f6f001`, bringing the total number of pairs to $N = \mathcal{S} \cdot 2^{79}$. Therefore, the data complexity of the attack is $\mathcal{S} \cdot 2^{80}$ chosen-plaintexts.



(a) Differential propagation in the key schedule.

(b) Key-recovery procedure of the 9-round related-key attack.

Fig. 6. 9-round related-key differential attack on HALFLOOP-96.

In the attack, an empty hash table $\mathbb{H}$ is created. For each output pair (O, O') returned by the encryption oracle, if the conditions

$$\Delta O[0\text{-}2] = \texttt{0x5af6f6},\ \Delta O[5] \oplus \Delta O[9] = \Delta O[6] \oplus \Delta O[10] = \texttt{0xf6}.$$

are fulfilled, the quadruple $(P, P', O[3, 4, 7, 11], O'[3, 4, 7, 11])$ will be inserted into $\mathbb{H}$ at index $\Delta O[8\text{-}10]$. Consequently, $\mathbb{H}$ contains approximately $N \cdot 2^{-40}$ quadruples, and each index $\Delta O[8\text{-}10]$ corresponds to approximately $N \cdot 2^{-64}$ quadruples. The index $\Delta O[8\text{-}10]$ that renders differential propagation of either `0xf6` $\rightarrow \Delta O[8] \oplus$ `ad` or `0xf6` $\rightarrow \Delta O[9]$ impossible for the S-box is then eliminated from $\mathbb{H}$. After this stage, there are approximately $2^{24} \cdot (127/256)^2 = 2^{21.98}$ indexes remaining in $\mathbb{H}$. The time complexity of this phase is dominated by the time to query the encryption oracle, which corresponds to line 3 of Algorithm 1 and is equivalent to $\mathsf{T}_{\mathsf{L3}} = \mathcal{S} \cdot 2^{79} \cdot 2 = \mathcal{S} \cdot 2^{80}$ 9-round encryptions.

For each index ΔO[8-10] in $\mathbb{H}$, we guess the value of $RK_9[4]$ and initialise an empty table $\mathbb{T}_1$. After deriving the value of $RK'_9[4] = RK_9[4] \oplus \Delta O[8] \oplus \texttt{5a}$, the value of $\Delta X_8[4]$ for each quadruple at index ΔO[8-10] can be computed.

Algorithm 1: 9-round related-key differential attack

```
1  Create $\mathcal{S} \cdot 2^{79}$ pairs $(P, P')$ from $\mathcal{S}$ structures
2  Initialise an empty hash table $\mathbb{H}$
3  Obtain the value of $(O, O')$ for each $(P, P')$ by querying the encryption oracle
4  if $\Delta O$[0-2] = 0x5af6f6 and $\Delta O[5] \oplus \Delta O[9] = \Delta O[6] \oplus \Delta O[10] =$ 0xf6 then
5      $(P, P', O[3,4,7,11], O'[3,4,7,11])$ is inserted into $\mathbb{H}$ at index $\Delta O$[8-10]
6  end
7  foreach index $\Delta O$[8-10] of $\mathbb{H}$ do
8      if 0xf6 $\rightarrow \Delta O[8] \oplus$ ad or 0xf6 $\rightarrow \Delta O[9]$ are impossible propagations then
9          Remove the index $\Delta O$[8-10] from $\mathbb{H}$
10     else
11         foreach 8-bit possible values of $RK_9[4]$ do
12             Initialise an empty table $\mathbb{T}_1$
13             Derive $RK'_9[4] = RK_9[4] \oplus \Delta O[8] \oplus$ 0x5a
14             foreach $(P, P', O[3,4,7,11], O'[3,4,7,11])$ at index $\Delta O$[8-10] do
15                 Compute $\Delta X_8[4]$
16                 if $\Delta X_8[4] =$ 0xad then
17                     Inserted $(P, P', O[3,7,11], O'[3,7,11])$ into table $\mathbb{T}_1$
18                 end
19             end
20             foreach 63 possible values of $\alpha'$ and 127 possible values of $\zeta$ do
21                 foreach 24-bit possible values of $RK_9[3,7,11]$ do
22                     Initialise an empty table $\mathbb{T}_2$
23                     Derive $RK'_9[3,7,11] = RK_9[3,7,11] \oplus (\alpha' \| (\alpha' \oplus \zeta) \| \zeta)$
24                     foreach $(P, P', O[3,7,11], O'[3,7,11])$ in $\mathbb{T}_1$ do
25                         Compute $\Delta X_8[3,7,11]$
26                         if $\Delta X_8[3] = \Delta X_8[7] = \Delta X_8[11] = \alpha' \oplus$ 0x01 then
27                             Inserted $(P, P')$ into table $\mathbb{T}_2$
28                         end
29                     end
30                     Count the number of pairs Ctr in $\mathbb{T}_2$
31                     if Ctr $\geqslant \tau$ then
32                         Derive candidates for $RK_0[4,5,8,10]$ with $(P, P')$ in $\mathbb{T}_2$
33                         Output $RK_0[4,5,8,10] \| RK_9[3,4,7,11] \| \alpha' \| \zeta \| \Delta$[8-10]
34                     end
35                 end
36             end
37         end
38     end
39 end
```

If $\Delta X_8[4] = \texttt{0xad}$, the quadruple $(P, P', O[3,7,11], O'[3,7,11])$ is inserted into table $\mathbb{T}_1$. The approximate number of quadruples in $\mathbb{T}_1$ is $N \cdot 2^{-64} \cdot 2^{-8} = N \cdot 2^{-72}$. This phase, which corresponds to line 14 of Algorithm 1, has a time complexity of $\mathsf{T}_{\mathsf{L14}} = 2^{21.98} \cdot 2^8 \cdot N \cdot 2^{-64} \cdot 2/12 = \mathcal{S} \cdot 2^{42.40}$ one-round encryptions.

Since the difference $\Delta RK_9[3,7,11]$ is related to undetermined values α' and ζ, the following attack should enumerate the values of α' and ζ. Noting that $\texttt{5a} \rightarrow \zeta$ is a possible propagation for the S-box, ζ can take on one of 127 possible values. Since $\texttt{ad} \rightarrow \alpha' \oplus \texttt{0x01}$ and $\alpha' \rightarrow \Delta O[10]$ must be possible propagations for the S-box, the probability that a random 8-bit vector validates the two constraints for the case of α' is $(127/256)^2 = 2^{-2.02}$. Therefore, α' has an average of 63 possible values. Then, for all 63 possible values of α' and 127 possible values of ζ, we estimate the value of $RK_9[3,7,11]$ and create an empty table $\mathbb{T}_2$. After deriving the values of $RK'_9[3] = RK_9[3] \oplus \alpha'$, $RK'_9[7] = RK_9[7] \oplus \alpha' \oplus \zeta$, and $RK'_9[11] = RK_9[11] \oplus \zeta$, it is possible to calculate the value of $\Delta X_8[3,7,11]$. If $\Delta X_8[3] = \Delta X_8[7] = \Delta X_8[11] = \alpha' \oplus \texttt{0x01}$, the quadruple in $\mathbb{T}_1$ will be inserted into $\mathbb{T}_2$. Consequently, $\mathbb{T}_2$ contains approximately $N \cdot 2^{-72} \cdot 2^{-24} = N \cdot 2^{-96}$ quadruples. This step, which corresponds to line 24 of Algorithm 1, has a time complexity of $\mathsf{T}_{\mathsf{L24}} = 2^{21.98} \cdot 2^8 \cdot 63 \cdot 127 \cdot 2^{24} \cdot N \cdot 2^{-72} \cdot 3 \cdot 2/12 = \mathcal{S} \cdot 2^{72.95}$ one-round encryptions.

We set a counter Cnt in order to remember the number of quadruples in $\mathbb{T}_2$. Based on the analysis presented above, the value of Cnt follows a binomial distribution with parameters $\mathcal{B}(N, p_0 = 2^{-90})$ for a correct key guess and $\mathcal{B}(N, p = 2^{-96})$ otherwise. The threshold τ is set to two correct pairs, and the success probability P_S is set to 90.00%. Using Eqn. (2), we determine $\mathcal{S} = 2^{12.96}$ and $\varepsilon_1 = 2^{-14.77}$. Therefore, there are $\varepsilon_1 \cdot 2^{21.98} \cdot 2^{32} \cdot 63 \cdot 127 = \varepsilon_1 \cdot 2^{66.95}$ candidates for $RK_9[3,4,7,11] \| \alpha' \| \zeta \| \Delta[8\text{-}10]$ that satisfy the condition at line 30 of Algorithm 1. Utilising the property of the four active S-boxes in the first round, as depicted in Fig. 6(b), and relying on right pairs, additional information about the key can be recovered. Take the S-box at $X_0[4]$ as an illustration. Since the input difference $\texttt{0x9a}$ must be propagated to the output difference $\texttt{0xdb}$, there are only four possible values for $X_0[4]$ and $X'_0[4]$, which are $\texttt{0x00}$, $\texttt{0x72}$, $\texttt{0x9a}$, and $\texttt{0xe8}$. This restriction allows us to screen out candidates for $RK_0[4]$ with a probability of 2^{-6}. Likewise, the constraints on $X_0[5]$, $X_0[8]$ and $X_0[10]$ yield a sieving probability of 2^{-18}. There are a total of $\varepsilon_1 \cdot 2^{66.95} \cdot 4^4 = \varepsilon_1 \cdot 2^{74.95}$ candidates for $RK_0[4,5,8,10] \| RK_9[3,4,7,11] \| \alpha' \| \zeta \| \Delta[8\text{-}10]$. This phase, corresponding to line 31 of Algorithm 1, has a maximal time complexity of $\mathsf{T}_{\mathsf{L31}} = \varepsilon_1 \cdot 2^{66.95}$ one-round encryptions. We recover equivalently $1/\varepsilon_1 + 6 \cdot 4 = 38.77$ bits of information about the key pair. As a result, the total time complexity of the attack is $\mathsf{T}_{\mathsf{L3}} + (\mathsf{T}_{\mathsf{L14}} + \mathsf{T}_{\mathsf{L24}} + \mathsf{T}_{\mathsf{L31}})/9 = 2^{92.96}$ 9-round encryptions. Given that the hash table $\mathbb{H}$ dominates memory consumption, the memory complexity of the attack is $2^{56.96}$ bytes.

Remark 1. We attempt to recover the remaining key bits as well. However, the time required to seek the remaining key bits exhaustively exceeds 2^{94}. The recovery of complete information about the key is an intriguing future endeavour.

6 Conclusion

This paper focuses on the differential distinguishers and related-key differential attacks on HALFLOOP-96. SAT problems are utilised to model the search for differential distinguishers. We use the SAT solver to determine the minimum number of active S-boxes and the maximum differential probability for the conventional, related-tweak, and related-key differential attack configurations. By applying the newly discovered 8-round related-key differential distinguisher, we launch a 9-round related-key differential attack against the cipher. The attack is weak-key and effective against 2^{94} key pairs with a specified difference. Although the attack does not pose a real security threat to HALFLOOP-96, the security margin of the cipher in the setting for related-key attacks is minimal. Consequently, care must be taken to avoid misuse.

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).

References

1. Interoperability and performance standards for medium and high frequency radio systems. United States Department of Defense Interface Standard MIL-STD-188-141D
2. Specification for the advanced encryption standard (aes). Federal Information Processing Standards Publication 197 (2001), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
3. Abdelkhalek, A., Sasaki, Y., Todo, Y., Tolba, M., Youssef, A.M.: MILP modeling for (large) s-boxes to optimize probability of differential characteristics. IACR Trans. Symmetric Cryptol. **2017**(4), 99–129 (2017). https://doi.org/10.13154/tosc.v2017.i4.99-129
4. Ankele, R., Kölbl, S.: Mind the gap - A closer look at the security of block ciphers against differential cryptanalysis. In: Cid, C., Jr., M.J.J. (eds.) Selected Areas in Cryptography - SAC 2018 - 25th International Conference, Calgary, AB, Canada, August 15-17, 2018, Revised Selected Papers. Lecture Notes in Computer Science, vol. 11349, pp. 163–190. Springer (2018). https://doi.org/10.1007/978-3-030-10970-7_8
5. Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings. Lecture Notes in Computer Science, vol. 537, pp. 2–21. Springer (1990). https://doi.org/10.1007/3-540-38424-3_1

6. Biryukov, A., Khovratovich, D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: Matsui, M. (ed.) Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings. Lecture Notes in Computer Science, vol. 5912, pp. 1–18. Springer (2009). https://doi.org/10.1007/978-3-642-10366-7_1
7. Biryukov, A., Khovratovich, D., Nikolic, I.: Distinguisher and related-key attack on the full AES-256. In: Halevi, S. (ed.) Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings. Lecture Notes in Computer Science, vol. 5677, pp. 231–249. Springer (2009). https://doi.org/10.1007/978-3-642-03356-8_14
8. Blondeau, C., Gérard, B., Tillich, J.: Accurate estimates of the data complexity and success probability for various cryptanalyses. Des. Codes Cryptogr. **59**(1-3), 3–34 (2011). https://doi.org/10.1007/s10623-010-9452-2
9. Boura, C., Coggia, D.: Efficient MILP modelings for sboxes and linear layers of SPN ciphers. IACR Trans. Symmetric Cryptol. **2020**(3), 327–361 (2020). https://doi.org/10.13154/tosc.v2020.i3.327-361
10. 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
11. 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
12. Dansarie, M., Derbez, P., Leander, G., Stennes, L.: Breaking HALFLOOP-24. IACR Trans. Symmetric Cryptol. **2022**(3), 217–238 (2022). https://doi.org/10.46586/tosc.v2022.i3.217-238
13. Kim, S., Hong, D., Sung, J., Hong, S.: Accelerating the best trail search on aes-like ciphers. IACR Trans. Symmetric Cryptol. **2022**(2), 201–252 (2022). https://doi.org/10.46586/tosc.v2022.i2.201-252
14. Lai, X., Massey, J.L., Murphy, S.: Markov ciphers and differential cryptanalysis. In: Davies, D.W. (ed.) Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings. Lecture Notes in Computer Science, vol. 547, pp. 17–38. Springer (1991). https://doi.org/10.1007/3-540-46416-6_2
15. Li, T., Sun, Y.: Superball: A new approach for MILP modelings of boolean functions. IACR Trans. Symmetric Cryptol. **2022**(3), 341–367 (2022). https://doi.org/10.46586/tosc.v2022.i3.341-367
16. 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. Sci. China Inf. Sci. **64**(5) (2021). https://doi.org/10.1007/s11432-018-9772-0
17. Liu, Y., Wang, Q., Rijmen, V.: Automatic search of linear trails in ARX with applications to SPECK and chaskey. In: Manulis, M., Sadeghi, A., Schneider, S.A. (eds.) Applied Cryptography and Network Security - 14th International Conference, ACNS 2016, Guildford, UK, June 19-22, 2016. Proceedings. Lecture Notes in Computer Science, vol. 9696, pp. 485–499. Springer (2016). https://doi.org/10.1007/978-3-319-39555-5_26
18. Matsui, M.: On correlation between the order of s-boxes and the strength of DES. In: Santis, A.D. (ed.) Advances in Cryptology - EUROCRYPT '94, Workshop on

the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings. Lecture Notes in Computer Science, vol. 950, pp. 366–375. Springer (1994). https://doi.org/10.1007/BFb0053451

19. 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
20. 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
21. Soos, M., Nohl, K., Castelluccia, C.: Extending SAT solvers to cryptographic problems. In: Kullmann, O. (ed.) Theory and Applications of Satisfiability Testing - SAT 2009, 12th International Conference, SAT 2009, Swansea, UK, June 30 - July 3, 2009. Proceedings. Lecture Notes in Computer Science, vol. 5584, pp. 244–257. Springer (2009). https://doi.org/10.1007/978-3-642-02777-2_24
22. Sun, B., Liu, Z., Rijmen, V., Li, R., Cheng, L., Wang, Q., AlKhzaimi, H., Li, C.: Links among impossible differential, integral and zero correlation linear cryptanalysis. In: Gennaro, R., Robshaw, M. (eds.) Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I. Lecture Notes in Computer Science, vol. 9215, pp. 95–115. Springer (2015). https://doi.org/10.1007/978-3-662-47989-6_5
23. 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
24. Sun, L., Wang, W., Wang, M.: More accurate differential properties of LED64 and midori64. IACR Trans. Symmetric Cryptol. **2018**(3), 93–123 (2018). https://doi.org/10.13154/tosc.v2018.i3.93-123