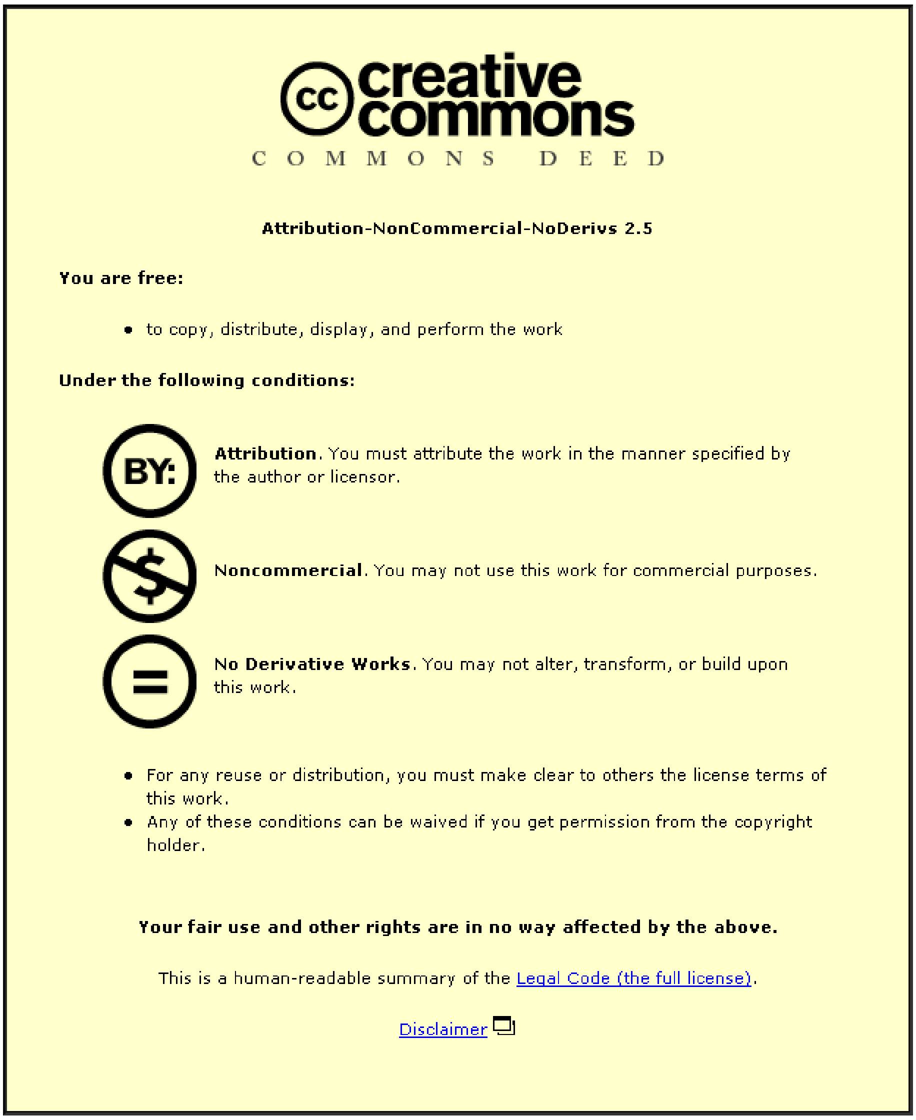
Advanced differential-style cryptanalysis of the NSA's skipjack block cipher



Advanced Differential-Style Cryptanalysis of the NSA's Skipjack Block Cipher

Jongsung Kim[1]* and Raphael C.-W. Phan[2]**

[1] Center for Information Security Technologies (CIST),
Korea University, Anam Dong, Sungbuk Gu, Seoul, Korea
joshep@cist.korea.ac.kr
[2] Electronic & Electrical Engineering Department,
Loughborough University, LE11 3TU, United Kingdom
R.Phan@lboro.ac.uk

Abstract. Skipjack is a block cipher designed by the NSA for use in US government phones, and commercial mobile and wireless products by AT&T. Among its initial implementations in hardware were the Clipper chip and Fortezza PC cards, which have since influenced the private communications market to be compatible with this technology. For instance, the Fortezza card comes in PCMCIA interface and is a very easy plug-n-play device to add on to mobile and wireless systems to provide encryption for wireless transmissions. Initially classified when it was first proposed, Skipjack was declassified in 1998 and sparked numerous security analyses from security researchers worldwide because it provides insight into the state-of-the-art security design techniques used by a highly secretive government intelligence agency such as the NSA. In this paper, commemorating a decade since Skipjack's public revelation, we revisit the security of Skipjack, in particular its resistance to advanced differential-style distinguishers. In contrast to previous work that considered conventional and impossible differential distinguishers, we concentrate our attention on the more recent advanced differential-style and related-key distinguishers that were most likely not considered in the original design objectives of the NSA. In particular, we construct first-known related-key impossible differential, rectangle and related-key rectangle distinguishers of Skipjack. Our related-key attacks (i.e., related-key miss-in-the-middle and related-key rectangle attacks) are better than all the previous related-key attacks on Skipjack. Finally, we characterize the strength of Skipjack against all these attacks and motivate reasons why, influenced by the Skipjack structure, some attacks fare better. What is intriguing about Skipjack is its simple key schedule and a structure that is a cross between conventional Feistel design principles and the unconventional use of different round types. This work complements past results on the security analysis of Skipjack and is hoped to provide further insight into the security of an NSA-designed block cipher; the only one publicly known to date.

Keywords: Block Ciphers, Skipjack, NSA, Distinguisher, Analysis, Related-Key Miss-in-the-Middle Attacks, Boomerang and Rectangle Attacks.

1 Introduction

Skipjack [56] is a 64-bit symmetric-key block cipher designed by the US National Security Agency (NSA). After Skipjack was designed, it was classified to be used in tamper-resistant Capstone and Clipper chips for US government purposes, e.g., voice, mobile and wireless communcations. What is intriguing about this cipher and what catches public attention to its design and analysis is that it was designed by mathematicians within the NSA, an agency highly notorious for its secrecy and the most advanced cipher design and analysis technology in the world. Moreover, the fact that it was designed and finalized in 1990, more than a decade after DES, means that it is expected that Skipjack be much more secure and resistant to known attacks. To allay initial public doubts [21, 62] of its security, a panel of 5 well-known cryptographers were asked to review its security [20] in

* The first author was supported by the Second Brain Korea 21 Project.

** Part of this work done while the author was with the Laboratoire de sécurité et de cryptographie (LASEC), Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland.

1993, and one of the conclusions made was:

"In summary, SKIPJACK is based on some of NSA's best technology. Considerable care went into its design and evaluation in accordance with the care given to algorithms that protect classified data."

Skipjack was declassified in 1998 [56], and immediately triggered several cryptanalytic results including [3, 4, 43]. In addition to the public speculation and distrust of Skipjack, the facts that it is designed with "alien" encryption technology by NSA, that it was initially classified but later made public, and that it consists of very simple round functions and a simple key schedule algorithm, have intrigued cryptanalysts [3, 4, 24, 26, 27, 43, 44, 54, 55, 61].

1.1 Outline of This Paper

In this paper we revisit the design and structure of Skipjack with respect to resistance against differential-style attacks. We particularly treat the existence of advanced differential-style distiguishers that can be used to mount attacks on reduced-round Skipjack variants.

In Sect. 2.1 we present the *related-key miss-in-the-middle* (RK-MisM) attack [58] on block ciphers as a natural related-key [1, 2, 59] counterpart of the conventional miss-in-the-middle (MisM) attack [5]. This is useful to exploit two (often short) related-key differentials into a longer related-key impossible differential that covers more rounds of the cipher. In general, whenever probability-one related-key differentials exist through two round sequences of a cipher, then the RK-MisM can be considered.

In Sect. 2.2 we unify all previous works on *boomerang*-style distinguishers [63, 32, 6, 57, 7, 8, 48, 37] and their related-key counterparts [36, 25, 38, 9, 10, 22, 53, 29, 35, 64, 46, 47, 49, 50, 23]. We highlight their similarities and differences for a better view of which attack variant is more suitable for a particular situation.

We also show for the first time[1] how amplified boomerang and rectangle distinguishers can be constructed by using only truncated differentials. Notice that all previous attacks [32, 39, 6–8] have the restriction [45] that differentials for the first half of the cipher must be conventional non-truncated types.

Sect. 3 is a brief one that describes Skipjack, the complementation properties of its G permutation, and also points out flaws in previous differential attacks of Skipjack in [26].

We present in Sect. 4 and 5 the first-known related-key miss-in-the-middle, rectangle and related-key rectangle distinguishers of Skipjack. Our rectangle attacks together with other attacks in [3, 44, 43, 26, 55] show that in the non-related-key setting, allowing the adversary to obtain sets of chosen texts of cardinality greater than 2 offers no added advantage over obtaining sets of chosen texts with cardinality 2 (a pair). In fact, conventional differential crypanalysis using pairs (cardinality 2) of chosen texts suffices; indeed the current best attack [4] on Skipjack is of this type.

Furthermore, our related-key attacks are better than all the previous related-key attacks on Skipjack [54, 55].

The best previous attack on Skipjack [4] was presented a decade ago, but since then no improvements have been reported and an attack on the full 32-round Skipjack remains elusive until now. This work is intended to summarize previous attacks on Skipjack variants, and simultaneously consider some further interesting properties and advanced distinguishers to provide more insight into its structure, and motivate continued public analysis of the NSA's design of Skipjack.

2 Advanced Differential-Style Attacks & Related-Key Counterparts

We discuss advanced differential-style distinguishers that make use of several short differentials to form long ones such as the impossible differential and boomerang-style distinguishers, and also discuss their related-key counterparts.

[1] We developed initial ideas for truncated amplified boomerangs in 2001 [57].

2.1 The Miss-in-the-Middle Attack

The *miss-in-the-middle* attack (the term was coined by Biham et al. in [5]), was first applied by Knudsen [42] to construct a 5-round impossible differential of the DEAL block cipher, which is a Feistel cipher. This concept was later generalized by Biham et al. [5] as a generic construction to build impossible differentials for ciphers of any structure. Consider a cipher E as a cascade, i.e., $E = E_1 \circ E_0$ such that for E_0 there exists a differential $(\alpha \rightarrow \beta)$ and for E_1 there exists a differential $(\gamma \rightarrow \delta)$, both with probability one, where $\beta \neq \gamma$. Both these are then used to form an *impossible differential* distinguisher, using the miss-in-the-middle technique:[2]

- `Chosen-Plaintext (CP) Query:`
  Obtain the encryption of a pair of plaintexts (P_1, P_2) such that $P_1 \oplus P_2 = \alpha$, and denote the corresponding ciphertexts by (C_1, C_2).
- Check whether $C_1 \oplus C_2 = \delta$ [Impossible Condition].

The impossible condition $(\alpha \not\rightarrow \delta)$ happens because $(\alpha \rightarrow \beta)$ always goes through E_0 and $(\gamma \rightarrow \delta)$ always goes through E_1 but since $\beta \neq \gamma$, thus $(\alpha \rightarrow \delta)$ is impossible. A plaintext pair $P_1 \oplus P_2 = \alpha$, and corresponding ciphertext pair $C_1 \oplus C_2 = \delta$ would form an impossible differential distinguisher. This was formed by a contradiction (miss) in the middle of the cipher, hence the name.

In practice, impossible differentials can be used by guessing their outer keys. That is, if the guessed outer keys cause impossible differentials, then they are discarded since the right key never cause impossible differentials.

Related-Key Miss-in-the-Middle Attack. The miss-in-the-middle attack is used to concatenate normal (non-related-key) differentials. It is natural to apply this technique to the *related-key* setting. We first remark that related-key differentials are in fact very similar to normal differentials. While the latter makes use of differences only in the input pair, the former uses differences not only in the input pair but also in the key pair. Differences in the key pair subsequently cause corresponding differences in the round-key pairs generated from the key pair. However, aside from this, differentials basically trace a difference value as it propagates through the cipher. Therefore, regardless of whether the difference comes from the input or from the key as well, we can treat and analyze these differentials in the same way. Therefore, the *related-key miss-in-the-middle (RK-MisM)* attack[3] is a related-key counterpart of the normal miss-in-the-middle attack [5], and can equally be applied to concatenate two probability-one related-key differentials such that they form a contradiction in the middle. The concatenation of the two differentials results in a related-key impossible differential.

2.2 The Boomerang, Amplified Boomerang and Rectangle Attacks

Wagner [63] considered a cipher $E = E_1 \circ E_0$ such that for E_0 (respectively E_1) there exists a differential $(\alpha \rightarrow \beta)$ with probability p (respectively $(\gamma \rightarrow \delta)$ with probability q). He then defined the *boomerang* distinguisher as follows:

- `Chosen-Plaintext (CP) Query:`
  Obtain ciphertexts (C_1, C_2) of a pair of plaintexts (P_1, P_2) such that $P_1 \oplus P_2 = \alpha$.
- `Adaptively-Chosen Ciphertext (ACC) Query:`
  Calculate $C_3 = C_1 \oplus \delta$ and $C_4 = C_2 \oplus \delta$, and obtain the decryption of the pair (C_3, C_4), thus (P_3, P_4).
- Check whether $P_3 \oplus P_4 = \alpha$ [Boomerang Condition].

The boomerang distinguisher uses the differential $(\alpha \rightarrow \beta)$ to cover E_0 in forward direction with respect to the pairs (P_1, P_2) but in backward direction with respect to the pairs (P_3, P_4); and the differential $(\gamma \rightarrow \delta)$ to cover E_1 in backward direction with respect to both (C_1, C_3) and (C_2, C_4).

[2] Note that not all impossible differentials are necessarily constructed via the miss-in-the-middle technique that uses two short differentials. Some other techniques include the shrinking technique [4], or simply using just one long differential that never results in a certain output difference.

[3] The idea of RK-MisM was independently introduced in [58] and [28]. Since then, it has also been used in [11].

The boomerang condition ($P_3 \oplus P_4 = \alpha$) happens because CP and ACC queries cause the *boomerang property* to occur in the middle of the cipher E:

$$\begin{aligned} E_0(P_3) \oplus E_0(P_4) &= E_0(P_1) \oplus E_0(P_2) \oplus E_0(P_1) \oplus E_0(P_3) \oplus E_0(P_2) \oplus E_0(P_4) \\ &= (E_0(P_1) \oplus E_0(P_2)) \oplus (E_1^{-1}(C_1) \oplus E_1^{-1}(C_3)) \oplus (E_1^{-1}(C_2) \oplus E_1^{-1}(C_4)) \\ &= \beta \oplus \gamma \oplus \gamma = \beta. \end{aligned}$$

This boomerang property holds with probability pq^2 since $E_0(P_1) \oplus E_0(P_2) = \beta$ with probability p and $E_1^{-1}(C_1) \oplus E_1^{-1}(C_3) = E_1^{-1}(C_2) \oplus E_1^{-1}(C_4) = \gamma$ with probability q^2. When this boomerang property occurs, we then have $P_3 \oplus P_4 = \alpha$ with probability p due to the differential ($\beta \to \alpha$) through E_0^{-1}, and thus for the cipher E, the total probability of the boomerang distinguisher, i.e., the probability of satisfying the boomerang condition, is $(pq)^2$. On the other hand, this boomerang condition is satisfied with probability 2^{-n} for a random permutation, where n is the block size. Hence, if $(pq)^2 >> 2^{-n}$, then this distinguisher can be used to effectively distinguish E from a random permutation.

In fact, the resultant probability of the boomerang distinguisher can be improved (see [63] Sect. 4) using all possible differentials for E_0 and E_1 such that β and γ are varied over all their possible values (as long as $\beta \neq \gamma$), i.e., the intermediate differences β and γ do not have to be fixed to any values, only α and δ need to be fixed. This refinement[4] increases the total probability to $(\hat{p}\hat{q})^2$, and to align with current naming convention would be more rightly called the *rectangled boomerang* distinguisher, where:

$$\hat{p} = \sqrt{\sum_{\beta} \texttt{Pr}^2[\alpha \to \beta]}, \quad \hat{q} = \sqrt{\sum_{\gamma} \texttt{Pr}^2[\gamma \to \delta]}. \tag{1}$$

One limitation of the boomerang is it requires adaptively-chosen ciphertexts, which works under a more restricted security model compared to more common known- and chosen-text attacks. To overcome this, Kelsey et al. [32] applied the birthday paradox technique by collecting many quartets (P_1, P_2, P_3, P_4) such that the boomerang-style condition is satisfied for at least a few such quartets. This was termed the *amplified boomerang* attack. The steps in constructing such a distinguisher are:

- `Chosen-Plaintext (CP) Query:`
  Obtain the encryption of a quartet of plaintexts (P_1, P_2, P_3, P_4) such that $P_1 \oplus P_2 = P_3 \oplus P_4 = \alpha$, and denote the corresponding ciphertexts by (C_1, C_2, C_3, C_4).
- Check whether $C_1 \oplus C_3 = C_2 \oplus C_4 = \delta$ [Amplified Boomerang Condition].

In this case, the amplified boomerang distinguisher uses the differential ($\alpha \to \beta$) to cover E_0 in the forward direction with respect to both the pairs (P_1, P_2) and (P_3, P_4); and the differential ($\gamma \to \delta$) to cover E_1 in the forward direction with respect to both the pairs (C_1, C_3) and (C_2, C_4).

The amplified boomerang condition ($C_1 \oplus C_3 = C_2 \oplus C_4 = \delta$) exists because when $E_0(P_1) \oplus E_0(P_3) = \gamma$ with some probability $\sigma = 2^{-n}$, then the amplified boomerang property occurs in the middle of the cipher E:

$$\begin{aligned} E_0(P_2) \oplus E_0(P_4) &= (E_0(P_1) \oplus E_0(P_2)) \oplus (E_0(P_3) \oplus E_0(P_4)) \oplus (E_0(P_1) \oplus E_0(P_3)) \\ &= \beta \oplus \beta \oplus \gamma = \gamma. \end{aligned}$$

This boomerang property holds with probability $2^{-n} \times p^2$ since $E_0(P_1) \oplus E_0(P_2) = E_0(P_3) \oplus E_0(P_4) = \beta$ with probability p^2 and $E_0(P_1) \oplus E_0(P_3) = \gamma$ with probability 2^{-n}. When this amplified boomerang property occurs, we then have $C_1 \oplus C_3 = C_2 \oplus C_4 = \delta$ with probability q^2 due to the differential ($\gamma \to \delta$) through E_1, and thus for the cipher E, the total probability of the amplified boomerang distinguisher, i.e., the probability of satisfying the amplified boomerang condition, is $2^{-n} \times (pq)^2$. Since this amplified boomerang condition is satisfied with probability 2^{-2n} for a random permutation, if $(2^{-n} \times (pq)^2) >> 2^{-2n}$, then this distinguisher effectively distinguishes E from a random permutation.

Similarly, the resultant probability of the amplified boomerang distinguisher can be improved [6] using all possible differentials for E_0 and E_1 such that β and γ are varied over all their possible

[4] Later called “rectangling” by Biham et al. [6].

values (as long as $\beta \neq \gamma$), i.e., the intermediate differences β and γ do not have to be fixed to any values, only α and δ need to be fixed. This rectangling refinement originally described by Wagner in [63] for the case of boomerang distinguishers, was adapted[5] by Biham et al. [6] to the amplified boomerang distinguisher case, and given the name "rectangle attack". For much clearer comparison with the original boomerang and amplified boomerang attacks, this would be more rightly called the *rectangled amplified boomerang* attack. The rectangle distinguisher has an increased total probability of $2^{-n} \times (\hat{p}\hat{q})^2$, where $\hat{p}$ and $\hat{q}$ are as previously defined in equation (1). (Note that the amplified boomerang condition can be $C_1 \oplus C_3 = C_2 \oplus C_4 = \delta$ or $C_1 \oplus C_4 = C_2 \oplus C_3 = \delta$, which allows to reduce an attack complexity by a factor of 2.) However, the crypto community has grown accustomed to the term "rectangle attacks" to mean either the original amplified boomerang attack in [32] or the later rectangle attacks in [6], henceforth unless otherwise stated we will just use "rectangle attacks" to refer to either one interchangibly.

Table 1 compares the differences between the boomerang attack variants. See Appendix C for a list of all known work on boomerang-style attacks.

Table 1. Comparing the Boomerang Attack Variants

Attack Variant	Differential Directions	Fixed Differences	Resultant Probability	Source
Boomerang	E_0, E_1, E_1, E_0^{-1}	$\alpha, \beta, \gamma, \delta$	$(pq)^2$	[63]
Rectangled Boomerang	E_0, E_1, E_1, E_0^{-1}	α, δ	$(\hat{p}\hat{q})^2$	[63]
Amplified Boomerang	E_0, E_0, E_1, E_1	$\alpha, \beta, \gamma, \delta$	$2^{-n} \cdot (pq)^2$	[32]
Rectangled Amplified Boomerang	E_0, E_0, E_1, E_1	α, δ	$2^{-n} \cdot (\hat{p}\hat{q})^2$	[6]

Extension: Using Only Truncated Differentials. Truncated differentials [41], unlike conventional non-truncated differentials [12, 13], do not necessarily have the same probability when going in reverse as when going forward. Thus when calculating the probability of a boomerang-style distinguisher based on the use of truncated differentials instead of non-truncated ones, more care is needed.

This special consideration for boomerang distinguishers with only truncated differentials was considered by Wagner in [63] Sect. 6. The boomerang property in the middle of E may not work since we are using truncated differences, where only a subset of w-bit (word) differences are fixed to '0' while remaining word differences are arbitrary and unknown. Let p_1 (respectively p_2) be a probability of a truncated differential $\alpha \to \beta$ for E_0 (respectively $\beta \to \alpha$ for E_0^{-1}) and q_1 (respectively q_2) be a probability of a truncated differential $\gamma \to \delta$ for E_1 (respectively $\delta \to \gamma$ for E_1^{-1}), where α, β, γ and δ all are non-empty difference sets. Then $E_0(P_1) \oplus E_0(P_2) = \beta_1 \in \beta$ with probability p_1, $E_1^{-1}(C_1) \oplus E_1^{-1}(C_3) = \gamma_1 \in \gamma$ with probability q_2 and $E_1^{-1}(C_2) \oplus E_1^{-1}(C_4) = \gamma_2 \in \gamma$ with probability q_2 and the boomerang property occurs in the middle of the cipher E:

$$\begin{aligned} E_0(P_3) \oplus E_0(P_4) &= E_0(P_1) \oplus E_0(P_2) \oplus E_0(P_1) \oplus E_0(P_3) \oplus E_0(P_2) \oplus E_0(P_4) \\ &= (E_0(P_1) \oplus E_0(P_2)) \oplus (E_1^{-1}(C_1) \oplus E_1^{-1}(C_3)) \oplus (E_1^{-1}(C_2) \oplus E_1^{-1}(C_4)) \\ &= \beta_1 \oplus \gamma_1 \oplus \gamma_2 = \beta_2 \in \beta, \end{aligned}$$

only if $\gamma_1 \oplus \gamma_2 = 0$ [truncated restriction] occurs with some probability ρ in words corresponding to zero word differences of β. Note that although the truncated differences β_1, β_2 (or γ_1, γ_2) are equal in the zero word differences, they may have different values in the non-zero arbitrary words. We call this the *truncated boomerang* distinguisher. Thus, the resultant probability of the boomerang distinguisher becomes $p_1 \cdot p_2 \cdot (q_2)^2 \times \rho$, where $\rho = 2^{-(m_\beta - m'_\gamma) \times w}$, and m_β is the number of w-bit zero word differences in β and m'_γ is the number of w-bit zero word differences in γ which

[5] To be clear, the first two improvements in [6] basically mean to count over all intermediate differences β and γ, and was already pointed out in [63]. The third improvement in [6] allows to optimize the probability of an amplified boomerang distinguisher, but it is very hard to do the exact calculation. Note that further improved attack algorithms for boomerang and rectangle attacks were later suggested in [7].

are in the positions of the zero word differences in β. The extra ρ factor is the effect of using truncated differentials instead of conventional non-truncated ones. See [15] for another example of how boomerang distinguishers of AES are constructed using only truncated differentials.

We now discuss how this applies to the amplified boomerang case. Although previous amplified boomerang attacks [32, 39], rectangle attacks [6–8] and related-key rectangle attacks [36, 25, 9, 10] have only used non-truncated differentials through the first half E_0 of the cipher, the same special truncated consideration applies when truncated differentials are used, and thus would be called the *truncated amplified boomerang* distinguisher (initiated in our earlier work [57]). As far as we know, using only truncated differentials to construct amplified boomerang distinguishers (and equally rectangled boomerang distinguishers) has not yet been considered before by other researchers. Here, the resultant probability of the truncated amplified boomerang distinguisher is $\sigma \times (p_1 q_1)^2 \times \rho$, where $\sigma = 2^{-m_\gamma \times w} < 2^{-n}$, $\rho = 2^{-(m_\gamma - m'_\beta) \times w}$, m_γ is the number of w-bit zero word differences in γ and m'_β is the number of w-bit zero word differences in β which are in the positions of the zero word differences in γ. In Sect. 5 we will demonstrate this by showing rectangle attacks using only truncated differentials through both halves of the cipher.

Related-Key Variants. The related-key boomerang attack was considered in [9], while the related-key rectangle (amplified boomerang) attack, first considered in [36] with 2 related keys, was later extended in [25, 10] to work with 4 related keys and in [9] with 256 related keys. The basic idea in [36] is to use *either* a conventional non-related-key differential *or* a related-key differential to cover E_0, and *both* non-related-key and related-key differentials to cover E_1. [25] used *only* related-key differentials to cover both E_0 and E_1. Meanwhile, [9] similarly used only related-key differentials to cover both E_0 and E_1, but they used structures of more related keys than [25], resulting in a higher probability of generating the required related-key rectangles. Refer to [36, 25, 9, 10] for illustrative descriptions of these.

3 Skipjack

The 64-bit block of Skipjack is divided into four 16-bit words. Eight A rounds and eight B rounds are alternated until full 32 rounds are achieved, and a constant round counter is used that is actually the round number (in the range 1 to 32). The transformation $G : \{0,1\}^{32} \times \{0,1\}^{16} \rightarrow \{0,1\}^{16}$ consists of a 4-round Feistel structure whose internal function $F : \{0,1\}^8 \rightarrow \{0,1\}^8$ is an 8×8 S-box (refer to Fig. 1 in Appendix A for the details of G).

The key schedule of Skipjack takes the 10-byte (80-bit) secret key, $K \in \{0,1\}^{80}$ and uses four bytes at a time for the G transformation in each round. Let $K = B_1B_2B_3B_4B_5B_6B_7B_8B_9B_{10}$ where $B_i \in \{0,1\}^8$ are the bytes of the key, K. Let $RK_i \in \{0,1\}^{32}$ be the ith round key. Then $RK_i = RK_{i \bmod 5}$ and specifically: $RK_1 = B_1B_2B_3B_4$, $RK_2 = B_5B_6B_7B_8$, $RK_3 = B_9B_{10}B_1B_2$, $RK_4 = B_3B_4B_5B_6$ and $RK_5 = B_7B_8B_9B_{10}$. After every 5 rounds, the cycle repeats, hence the key schedule of Skipjack appears to have a periodicity of 5 rounds. Fortunately, this does not make it susceptible to the slide attacks [18, 19] due to the different round types (A, B) used. See Fig. 2 in Appendix A for A- and B-round of Skipjack.

3.1 Complementation Properties of the G Permutation

We describe the complementation properties of the G permutation within the round functions, which are essential in our attacks on Skipjack. We first define the following:

- I_j^i: j-th 16-bit input value of the i-th round ($j = 1, 2, 3, 4$ and $i = 1, 2, \cdots, 32$).
- a: an arbitrary fixed nonzero 16-bit value ($a \neq 0$).
- b_i: an arbitrary 16-bit value such that $b_i \neq a$.
- c_i: an arbitrary nonzero 16-bit value ($c_i \neq 0$).
- d_i: an arbitrary 16-bit value.
- $\overline{x}$: a 16-bit value (x_2, x_1), containing swapped halves of $x = (x_1, x_2)$, where x_1 and x_2 are 8-bit values.

The $G : \{0,1\}^{32} \times \{0,1\}^{16} \rightarrow \{0,1\}^{16}$ permutation has $2^{16}-1$ complementation properties [3]. We denote as $I = (I_L, I_R) \in (\{0,1\}^8)^2$ and $O = (O_L, O_R) \in (\{0,1\}^8)^2$ the input and output of the G permutation, respectively. Then for any $KR_1 = (k_1, k_2) \in (\{0,1\}^8)^2, KR_2 = (k_3, k_4) \in (\{0,1\}^8)^2$ and nonzero $c_i = (c_{i,1}, c_{i,2}) \in (\{0,1\}^8)^2$, it has been proven that:

Theorem 1 [3]: Let $KR_1' = KR_1 \oplus c_i,\ KR_2' = KR_2 \oplus c_i,\ O = G_{(KR_1, KR_2)}(I)$ and $O' = G_{(KR_1', KR_2')}(I')$. Then $I' = I \oplus \overline{c_i}$ if and only if $O' = O \oplus \overline{c_i}$.

Corollary 1 [3]: Let $KR_1' = KR_1 \oplus c_i,\ KR_2' = KR_2 \oplus c_i,\ O = G_{(KR_1, KR_2)}(I)$ and $O' = G_{(KR_1', KR_2')}(I')$. Then $I' \neq I \oplus \overline{c_i}$ if and only if $O' \neq O \oplus \overline{c_i}$.

See Fig. 1 in Appendix A for a schematic description of the complementation properties of the G permutation.

3.2 Flaws in Differential Analysis of Skipjack

Recall that [24] reported flaws in the differential and boomerang attacks of Skipjack made in [43]. Here, we discuss further flaws in other previous differential attacks of Skipjack made in [26]. In [26] the differential attack has been mounted on 21, 24 and 26 rounds of Skipjack. In the 21-round differential attack, plaintext pairs with arbitrary non-zero differences have been used, while the 24- and 26-round differential attacks have both exploited plaintext pairs with a special difference which induces the best differential probability for the first round. In their analysis it has been claimed that all these plaintext pairs could extract about 2^{16} keys in the first round alike. However, it is not true. In fact, the number of keys which can be extracted in the first round depends only on the probability of a first-round differential considered in the attacks. More precisely, $|\mathcal{K}_1| = 2^{32} \cdot p$, where $\mathcal{K}_1$ is a set of extracted keys in the first round and p is the probability of a first-round differential (this property will be used in our analysis of Skipjack). It means that a plaintext difference can determine $|\mathcal{K}_1|$. Therefore, in their 24- and 26-round differential attacks, $|\mathcal{K}_1|$ is larger than 2^{16}, i.e., $2^{32} \cdot 2^{-10.42} = 2^{21.58}$ since the best one-round differential probability is $2^{-10.42}$ [3]. This fact makes infeasible to distinguish the right key from wrong keys of the 24- and 26-round Skipjack. Hence, their 24- and 26-round Skipjack attacks do not work.

4 Related-Key Miss-in-the-Middle Attacks on Skipjack

We exploit Theorem 1 and Corollary 1 to construct 19-round related-key impossible differentials. Theorem 1 states that given a pair of inputs, I and I' to G with the input difference $\Delta_I = I \oplus I' = \overline{a}$, if I is transformed through G with the round key $RK = (KR_1, KR_2) \in (\{0,1\}^{16})^2$ while I' is transformed through G with the round key $RK' = (KR_1 \oplus a, KR_2 \oplus a) \in (\{0,1\}^{16})^2$, then the difference is preserved at the output of G, namely $\Delta_O = O \oplus O' = \overline{a}$. Since G is a permutation, Corollary 1 states that $\Delta_I \neq \overline{a}$ if and only if $\Delta_O \neq \overline{a}$.

If $\Delta K = K \oplus K' = (a,a,a,a,a) \in (\{0,1\}^{16})^5$ and plaintext difference, $\Delta P = P \oplus P' = (\overline{a},0,0,0) \in (\{0,1\}^{16})^4$, then the difference after three A-rounds, where $1r_A$ denotes one A-round encryption, is:

$$(\overline{a},0,0,0) \overset{1r_A}{\rightarrow} (\overline{a},\overline{a},0,0) \overset{1r_A}{\rightarrow} (\overline{a},\overline{a},\overline{a},0) \overset{1r_A}{\rightarrow} (\overline{a},\overline{a},\overline{a},\overline{a}). \tag{2}$$

Tracing the propagation of the difference through 8 B-rounds gives:

$$(\overline{a},\overline{a},\overline{a},\overline{a}) \overset{1r_B}{\rightarrow} (\overline{a},\overline{a},0,\overline{a}) \overset{1r_B}{\rightarrow} (\overline{a},\overline{a},0,0) \overset{1r_B}{\rightarrow} (0,\overline{a},0,0) \overset{1r_B}{\rightarrow} (0,\overline{b_1},\overline{a},0)$$

$$\overset{1r_B}{\rightarrow} (0,\overline{b_2},\overline{b_1},\overline{a}) \overset{1r_B}{\rightarrow} (\overline{a},\overline{b_3},\overline{b_2},\overline{b_1}) \overset{1r_B}{\rightarrow} (\overline{b_1},\overline{a},c_1,\overline{b_2}) \overset{1r_B}{\rightarrow} (\overline{b_2},\overline{b_4},c_2,c_1). \tag{3}$$

The couple $\{(\overline{a},0,0,0),(\overline{b_2},\overline{b_4},c_2,c_1)\}$ is a probability-one 11-round related-key differential that states that given an input difference $(\overline{a},0,0,0)$, the output difference is always of the form $(\overline{b_2},\overline{b_4},c_2,c_1)$ after 3 A-rounds and 8 B-rounds, hereby denoted as $3r_A||8r_B$.

Now consider from the other end, a ciphertext difference, $\Delta C = C \oplus C' = (0, \overline{a}, \overline{a}, d_1) \in (\{0,1\}^{16})^4$. Tracing the propagation of the ciphertext difference backwards through 8 inverse A-rounds (denoted as $8r_A^{-1}$) gives a probability-one related-key differential of the form:

$$(0, \overline{a}, \overline{a}, d_1) \xrightarrow{1r_A^{-1}} (\overline{a}, \overline{a}, d_1, \overline{a}) \xrightarrow{1r_A^{-1}} (\overline{a}, d_1, \overline{a}, 0) \xrightarrow{1r_A^{-1}} (d_2, \overline{a}, 0, d_3) \xrightarrow{1r_A^{-1}} (\overline{a}, 0, d_3, d_4)$$

$$\xrightarrow{1r_A^{-1}} (\overline{b_1}, d_3, d_4, \overline{a}) \xrightarrow{1r_A^{-1}} (d_5, d_4, \overline{a}, d_6) \xrightarrow{1r_A^{-1}} (d_7, \overline{a}, d_6, d_8) \xrightarrow{1r_A^{-1}} (\overline{a}, d_6, d_8, d_9). \qquad (4)$$

Theorem 2: There exists a 19-round related-key impossible differential through $3r_A||8r_B||8r_A$ of the form $\{\Delta P, \Delta C\} = \{(\overline{a}, 0, 0, 0), (0, \overline{a}, \overline{a}, d_1)\}$, where $\Delta K = (a, a, a, a, a) \in (\{0,1\}^{16})^5$.

Proof of Theorem 2: From Eq. (2) and Eq. (3), given $\Delta P = (\overline{a}, 0, 0, 0)$, then after $3r_A||8r_B$, the difference is always of the form $(\overline{b_2}, \overline{b_4}, c_2, c_1)$. However, Eq. (4) states that given $\Delta C = (0, \overline{a}, \overline{a}, d_1)$, then after $8r_A^{-1}$, the difference is always of the form $(\overline{a}, d_6, d_8, d_9)$. Since the first word of $(\overline{b_2}, \overline{b_4}, c_2, c_1)$ is $\overline{b_2} \neq \overline{a}$ but the first word of $(\overline{a}, d_6, d_8, d_9)$ is $\overline{a}$, then we obtain a contradiction, so a plaintext difference, $\Delta P = (\overline{a}, 0, 0, 0)$ will never cause a ciphertext difference, $\Delta C = (0, \overline{a}, \overline{a}, d_1)$ after $3r_A||8r_B||8r_A$. □

From the 19-round related-key impossible differential in Theorem 2, we can construct another similar related-key impossible differential through $8r_B||8r_A||3r_B$, from the fact that the structure of r_A is the same as that of r_B^{-1}.

Corollary 2: There exists a 19-round related-key impossible differential through $8r_B||8r_A||3r_B$ of the form $\{\Delta P, \Delta C\} = \{(\overline{a}, 0, d_1, \overline{a}), (0, \overline{a}, 0, 0)\}$, where $\Delta K = (a, a, a, a, a) \in (\{0,1\}^{16})^5$.

4.1 The Attacks

The 19-round related-key impossible differential in Theorem 2 can be used to mount a related-key impossible differential attack on Skipjack reduced to 22 rounds, from the 4-th round to the 25-th round, namely $5r_A||8r_B||8r_A||1r_B$. Essentially, we apply this related-key impossible differential to the middle 19 rounds, namely $3r_A||8r_B||8r_A$. Then, we extract round keys, RK_4, RK_5 and RK_{25} at the outer rounds that satisfy the impossible differential. Since the right key cannot hold the impossible differential, the extracted round keys are wrong keys and hence discarded.

In order to induce the input difference $(\overline{a}, 0, 0, 0)$ and the output difference $(0, \overline{a}, \overline{a}, d_1)$ of the 19-round related-key impossible differential, we require a plaintext pair whose difference is of the form $(\overline{b_1}, 0, \overline{a}, \overline{b_2})$ and the corresponding ciphertext difference is of the form $(d_1, \overline{b_3}, \overline{a}, \overline{a})$. Once we get such a plaintext pair, we see that the input differences to G are $\overline{b_1}$ and $\overline{b_2}$ for rounds 4 and 5 which might cause a zero output difference with probability 2^{-16}, respectively, and the input difference to G^{-1} is $\overline{b_3}$ for round 25 which might cause a zero output difference[6] with probability 2^{-16}. Hence, after $2r_A$ in the first we would get a difference $(\overline{a}, 0, 0, 0)$ with probability 2^{-32} and after $1r_B^{-1}$ in the last a difference $(0, \overline{a}, \overline{a}, d_1)$ with probability 2^{-16}. It follows that for each desired plaintext pair we can extract wrong key candidates by a fraction of 2^{-48} for round keys $RK_4 = (k_3, k_4, k_5, k_6)$, $RK_5 = (k_7, k_8, k_9, k_{10})$ and $RK_{25} = (k_7, k_8, k_9, k_{10})$. Our attack then follows:

1. Obtain a structure of 2^{32} plaintext tuples, (P, P') such that $P = (x, y, z, w)$ and $P' = (x', y, z \oplus \overline{a}, w')$ where x, w, x' and w' are all 2^{16} possible values, and y, z are fixed constants. From these we can form about 2^{64} pairs such that $P \oplus P' = (\overline{b_1}, 0, \overline{a}, \overline{b_2})$, and that would satisfy the $(\overline{a}, 0, 0, 0)$ difference after $2r_A$ rounds with probability 2^{-32}. Obtain $2^{20} - 1$ other such structures of plaintext tuples by fixing the constants (y, z) to other values. Therefore, we get about $2^{64} \times 2^{20} = 2^{84}$ such pairs with the plaintext difference $(\overline{b_1}, 0, \overline{a}, \overline{b_2})$.
2. Obtain the encryptions of P under the key, K, and the encryptions of P' under $K' = K \oplus (a, a, a, a, a)$, and denote the corresponding ciphertexts by C and C', respectively.

[6] Note that we are dealing here not only with a difference $\overline{b_i}$ at the input or output of G but also a difference (a, a) in the round key used in G. Therefore, an input or output difference, b_i could also cause a zero output or input difference. This is in contrast to analysis in [3, 4] where there was only a difference at the input to G but no difference in the round keys.

3. For each of the 2^{84} pairs, choose only those pairs with the ciphertext difference, $C \oplus C' = (d_1, \overline{b_3}, \overline{a}, \overline{a})$. We expect about $2^{84} \times 2^{-32} = 2^{52}$ pairs to remain.
4. Initialize 2^{64} counters of keys $(k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10})$ with 0.
5. For each of 2^{52} remaining pairs (P, P') whose difference is $(\overline{b_1}, 0, \overline{a}, \overline{b_2})$:
   (a) (In round 4) Extract RK_4 which satisfy a related-key differential $\overline{b_1} \xrightarrow{G} 0$, and keep $(k_3, k_4, k_5, k_6, I_1^5)$ in a list, where I_1^5 is the first input value of the 5-th round computed from k_3, k_4, k_5, k_6 and P. Since the related-key differential holds with probability 2^{-16} on average, about 2^{16} entries will be kept in the list. We denote this list by $\mathcal{L}1$.
   (b) (In round 5) For each of I_1^5 in $\mathcal{L}1$, extract RK_5 which satisfy a related-key differential $\overline{b_2} \xrightarrow{G} 0$. Keep in a list $(k_7, k_8, k_9, k_{10}, I_1^5)$ for an arbitrary fixed I_1^5 in $\mathcal{L}1$. We denote this list by $\mathcal{L}2$. Due to the complementation properties of G, $\mathcal{L}2$ can cover all possible pairs (RK_5, I_1^5). Since the related-key differential used in round 5 also holds with probability 2^{-16}, about 2^{16} entries will be kept in $\mathcal{L}2$, but it covers about $2^{16} \times 2^{16} = 2^{32}$ entries.
   (c) Join the two lists $\mathcal{L}1$ and $\mathcal{L}2$ into a list of the form $(k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10}, I_1^5)$. We denote this joint list by $\mathcal{L}3$. About 2^{16} entries will be kept in $\mathcal{L}3$, but it covers 2^{32} entries.
   (d) (In round 25) For each of (k_7, k_8, k_9, k_{10}) in $\mathcal{L}3$, check if the ciphertext pair goes to the $(0, \overline{a}, \overline{a}, d_1)$ difference through the inverse of round 25. Since this is a 16-bit restriction, about 2^{16} $(k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10})$ will be suggested for each plaintext pair. Increase by 1 the counters of the suggested keys.
6. For each of the 64-bit subkeys whose counters are 0, do an exhaustive search for the remaining 16 key bits using trial encryption.

Steps 1 and 2 require the encryptions of 2^{20} structures of 2^{33} plaintexts under the related keys, (K, K'). Therefore, we need $2^{33} \times 2^{20} = 2^{53}$ related-key chosen-plaintext (RK-CP) queries. The memory complexity of this attack is dominated by Step 4, which requires 2^{64} 1-bit counters, equivalently 2^{61} bytes of memory. However, if we use (k_3, k_4) as the index of the iteration of Step 5 and we run Step 6 in Step 5, the memory complexity of this attack can be decreased down to 2^{45} bytes of memory.

We can complete Steps 5-(a), 5-(b) and 5-(d) for each plaintext pair with 2^{16} G computations using the differential distribution table of F and the complementation properties of G. In Step 5-(d) the probability that each wrong key is suggested is about 2^{-48}, so the expectation of the number of counters whose values are 0 is about $2^{64}(1-2^{-48})^{2^{52}} \approx 2^{40.92}$. It follows that Step 6 requires $2^{40.92} \times 2^{16} \times (1/2) = 2^{55.92}$ 22-round Skipjack encryptions on average. Hence, the overall time complexity of this attack is about $2^{52} \times 3 \times 2^{16} \times (1/22) = 2^{65.12}$ 22-round Skipjack encryptions.[7]

5 Rectangle Attacks on Skipjack

In this section, we demonstrate how rectangle attacks can be mounted based only on truncated differentials through both E_0 and E_1. We first give some rectangle distinguishers.

Theorem 3: There exists a 19-round rectangle distinguisher through $4r_A||8r_B||7r_A$ of the form $\{\alpha, \delta\} = \{(0, c_1, 0, 0), (c_2, c_2, 0, 0)\}$ with probability 2^{-79}, where c_1 and c_2 are arbitrary non-zero differences.

Proof of Theorem 3: Let $E_0 = 4r_A||8r_B$ and $E_1 = 7r_A$. Use a 12-round probability-one truncated differential $\{\alpha, \beta\} = \{(0, c_1, 0, 0), (c_3, c_4, c_5, 0)\}$ to cover E_0, and a 7-round truncated differential $\{\gamma, \delta\} = \{(0, c_6, c_7, 0), (c_2, c_2, 0, 0)\}$ to cover E_1 with probability 2^{-16}, where c_i are all arbitrary non-zero differences.

This can be used to form a rectangle distinguisher. When we have $\{\alpha, \beta\} = \{(0, c_1, 0, 0), (c_3, c_4, c_5, 0)\}$ going through both E_0 with probability one for the pairs (P_1, P_2) and (P_3, P_4), we then get with

[7] Note that if we use a less amount of plaintext structures in this attack, the time complexity of Step 6 is increased rapidly. For instance, if we use 2^{19} plaintext structures, Step 6 requires $2^{67.45}$ 22-round Skipjack encryptions.

probability $\sigma \approx 2^{-32}$ that $E_0(P_1) \oplus E_0(P_3) = \gamma_1 \in \{(0, c_6, c_7, 0)\} = \{\gamma\}$. Let $\beta_1 = (c'_3, c'_4, c'_5, 0)$, $\beta_2 = (c''_3, c''_4, c''_5, 0) \in \{\beta\}$ and $\gamma_1 = (0, c'_6, c'_7, 0) \in \{\gamma\}$; thus the boomerang property in the middle, i.e.

$$\begin{aligned}
\gamma_2 = E_0(P_2) \oplus E_0(P_4) &= (E_0(P_1) \oplus \beta_1) \oplus (E_0(P_3) \oplus \beta_2) \\
&= E_0(P_1) \oplus E_0(P_3) \oplus \beta_1 \oplus \beta_2 \\
&= \gamma_1 \oplus \beta_1 \oplus \beta_2 \\
&= (0, c'_6, c'_7, 0) \oplus (c'_3, c'_4, c'_5, 0) \oplus (c''_3, c''_4, c''_5, 0) \\
&= (c'_3 \oplus c''_3, c'_6 \oplus c'_4 \oplus c''_4, c'_7 \oplus c'_5 \oplus c''_5, 0) \in \{\gamma\}.
\end{aligned}$$

only if $c'_3 \oplus c''_3 = 0$, $c'_6 \oplus c'_4 \oplus c''_4 \neq 0$ and $c'_7 \oplus c'_5 \oplus c''_5 \neq 0$ with probability $\rho \approx 2^{-16}$. Thus $C_1 \oplus C_3,\ C_2 \oplus C_4 \in \{\delta\}$ with probability $(2^{-16})^2$ due to the differential $(\gamma \to \delta)$ through E_1. The resultant probability is thus $\sigma \times (p_1 q_1)^2 \times \rho \approx 2^{-32} \times (1 \times 2^{-16})^2 \times 2^{-16} = 2^{-80}$. This probability can be also applied to $C_1 \oplus C_4,\ C_2 \oplus C_3 \in \{\delta\}$ and thus the 19-round rectangle distinguisher has a probability of 2^{-79}, compared to the probability of 2^{-95} that it would occur for a random permutation. □

Similarly, there is another 19-round related-key rectangle distinguisher through the 19 rounds $4r_B^{-1}||8r_A^{-1}||7r_B^{-1}$.

Corollary 3: There exists a 19-round rectangle distinguisher through $4r_B^{-1}||8r_A^{-1}||7r_B^{-1}$ of the form $\{\alpha, \delta\} = \{(c_1, 0, 0, 0), (c_2, c_2, 0, 0)\}$ with probability 2^{-79}, where c_i are arbitrary non-zero differences.

5.1 The Attacks

The 19-round rectangle distinguisher in Theorem 3 can be used to attack Skipjack reduced to 23 rounds, from the 1-st round to the 23-th round, namely $8r_A||8r_B||7r_A$. We apply this distinguisher to the last 19 rounds, $4r_A||8r_B||7r_A$, and retrieve round keys, RK_1, RK_2, RK_3 and RK_4 in the first 4 rounds, $4r_A$.

To induce an input difference of the form $(0, c_1, 0, 0)$ of the 19-round rectangle distinguisher we require a plaintext pair whose difference is of the form $(c_4, c_3, 0, c_1)$. Once we get such a pair, we see in the first $4r_A$:

$$(c_4, c_3, 0, c_1) \overset{1r_A}{\to} (0, c_1, c_3, 0) \overset{1r_A}{\to} (0, 0, c_1, c_3) \overset{1r_A}{\to} (c_3, 0, 0, c_1) \overset{1r_A}{\to} (0, c_1, 0, 0) \qquad (5)$$

with a probability of approximately 2^{-32}. This is due to the required differential conditions $c_4 \overset{G}{\to} c_1$ and $c_3 \overset{G}{\to} c_1$ in rounds 1 and 4, respectively. However, if we use $c_1 = 0||52_x$ and $c_3 = c_4 = f5_x||0$, we can increase the probability[8] of Eq. (5) up to $2^{-20.84}$, which allows us to decrease the time complexity of the attack. It follows that for each two plaintext pairs (P_1, P_2) and (P_3, P_4) (i.e, one quartet) such that $P_1 \oplus P_2 = P_3 \oplus P_4 = (f5_x||0, f5_x||0, 0, 0||52_x)$ we can extract the right subkeys $RK_1 = (k_1, k_2, k_3, k_4)$, $RK_2 = (k_5, k_6, k_7, k_8)$, $RK_3 = (k_9, k_{10}, k_1, k_2)$ and $RK_4 = (k_3, k_4, k_5, k_6)$ with probability $2^{-41.68}$:

1. Obtain encryptions of $2^{61.84}$ plaintext pairs whose differences are all $(f5_x||0,\ f5_x||0, 0, 0||52_x)$. From these we can form $2^{122.68}$ plaintext quartets $((P_1, P_2), (P_3, P_4))$ such that $P_1 \oplus P_2 = P_3 \oplus P_4 = (f5_x||0, f5_x||0, 0, 0||52_x)$. Denote the corresponding ciphertext quartets $((C_1, C_2), (C_3, C_4))$.
2. Choose plaintext quartets such that $C_1 \oplus C_3$ and $C_2 \oplus C_4$ (or $C_1 \oplus C_4$ and $C_2 \oplus C_3$) are of the form $(c_2, c_2, 0, 0)$. Since it gives two 96-bit filtering conditions for each ciphertext quartet, about $2^{122.68} \times 2^{-95} = 2^{27.68}$ plaintext quartets will remain after this step.
3. Initialize 2^{80} counters of keys with 0.
4. For each of the remaining $2^{27.68}$ plaintext quartets $((P_1, P_2), (P_3, P_4))$:

[8] In [3] it was shown that differential $f5_x||0 \overset{G}{\to} 0||52_x$ is the best possible differential of G, which holds with probability $48/2^{16} = 2^{-10.42}$. Besides this, there exist several other forms of best differentials of G with the same probability.

(a) (In round 1) Extract $2^{32} \times 2^{-10.42} = 2^{21.58}$ RK_1 which satisfy a differential $f5_x||0 \xrightarrow{G} 0||52_x$ for (P_1, P_2). For each of the extracted $2^{21.58}$ RK_1, check if (P_3, P_4) satisfies differential $f5_x||0 \xrightarrow{G} 0||52_x$. If so, keep $(k_1, k_2, k_3, k_4, I_1^2, I_1'^2)$ in a list, where I_1^2 and $I_1'^2$ are the first 16-bit input values of the second round for (P_1, P_2, RK_1) and (P_3, P_4, RK_1), respectively. Since the differential holds with probability $2^{-10.42}$, about $2^{11.16}$ entries will be kept in the list. Denote this list by $\mathcal{L}1$.

(b) (In round 4) For each of all possible 2^{16} input pairs of G, $(I_1^4, I_1^4 \oplus f5_x||0)$, extract $2^{32} \times 2^{-10.42} = 2^{21.58}$ RK_4 which satisfy a differential $f5_x||0 \xrightarrow{G} 0||52_x$. Keep in a list $(k_3, k_4, k_5, k_6, I_1^4)$ for an arbitrary fixed I_1^4. Denote this list by $\mathcal{L}2$. Due to the complementation properties of G, $\mathcal{L}2$ can cover all possible pairs (RK_4, I_1^4). So $2^{21.58}$ entries will be kept in $\mathcal{L}2$, but it covers $2^{16} \times 2^{21.58} = 2^{37.58}$ entries.

(c) Join the two lists $\mathcal{L}1$ and $\mathcal{L}2$ into a list of the form $(k_1, k_2, k_3, k_4, k_5, k_6, I_1^2, I_2^4)$, where I_2^4 are the second 16-bit input values of the fourth round calculated by $(I_1^4, I_1^4 \oplus f5_x||0)$ and (P_1, P_2) (the values $I_1'^2$ in $\mathcal{L}1$ are not used in this step, but they will be used in Step 4-(e)). We denote this joint list by $\mathcal{L}3$. Since $\mathcal{L}1$ and $\mathcal{L}2$ have two 8-bit values k_3 and k_4 in common, about $2^{11.16} \times 2^{21.58} \times 2^{-16} = 2^{16.74}$ entries will be kept in $\mathcal{L}3$, but it covers $2^{16} \times 2^{16.74} = 2^{32.74}$ entries due to the complementation properties of G.

(d) (In rounds 2 and 3) For each of all possible $2^{32.74}$ entries in $\mathcal{L}3$, encrypt the first half of round 2 using k_5, k_6 and I_1^2 and decrypt the second half of round 3 using k_1, k_2 and I_2^4, and extract k_7, k_8, k_9, k_{10} using these encrypted and decrypted values. Keep in a list all extracted values k_7, k_8, k_9, k_{10} together with $k_1, k_2, k_3, k_4, k_5, k_6$. We denote this list by $\mathcal{L}4$. Since each possible entry in $\mathcal{L}3$ produces 2^{16} (k_7, k_8, k_9, k_{10}), about $2^{32.74} \times 2^{16} = 2^{48.74}$ keys will be kept in $\mathcal{L}4$.

(e) Perform Steps 4-(c) and 4-(d) for $I_1'^2$ and (P_3, P_4) to get $\mathcal{L}'3$ and $\mathcal{L}'4$. Similarly, about $2^{48.74}$ keys will be kept in $\mathcal{L}'4$.

(f) Increase by 1 the counters of the keys in both $\mathcal{L}4$ and $\mathcal{L}'4$ (note that this can be done efficiently by sorting $\mathcal{L}4$ and $\mathcal{L}'4$ by $k_1 \sim k_6$). For each plaintext quartet, about $2^{32.74} \times (2^{16})^2 \times 2^{-32} = 2^{32.74}$ counters of keys will be increased by 1 (note that this is computed based on the fact that for each of $2^{32.74}$ $(k_1, \cdots, k_6)$ in both $\mathcal{L}4$ and $\mathcal{L}'4$, 2^{16} (k_7, k_8, k_9, k_{10}) are suggested in each of $\mathcal{L}4$ and $\mathcal{L}'4$). Keep in a list keys whose counters are larger than or equal to 2. We denote this list by $\mathcal{K}$.

5. For each of the keys in $\mathcal{K}$ do an exhaustive search using trial encryption.

Step 1 requires the encryptions of $2^{62.84}$ plaintexts, and thus we need $2^{62.84}$ chosen-plaintext (CP) queries. Step 2 requires negligible effort (it can be done efficiently by sorting ciphertexts by the last two 16-bit values). The memory complexity of this attack is dominated by Step 3, which requires 2^{80} 2-bit counters, equivalently 2^{78} bytes of memory.

Step 4-(a) can be done efficiently using the differential distribution table of F, so we can complete Step 4-(a) for each plaintext quartet with $2 \times 2^{16} = 2^{17}$ G computations. Due to the complementation properties of G, we can complete Step 4-(b) with a similar amount of computations as Step 4-(a), namely, it requires 2^{16} G computations for each pair in a plaintext quartet. Step 4-(c) can be done efficiently by sorting the subkeys by k_3, k_4, so Step 4-(c) requires negligible effort. Since for each of all possible entries in $\mathcal{L}3$, 2^{16} G computations are needed to get k_7, k_8, k_9, k_{10}, the time complexity of Step 4-(d) is thus about $2^{32.74} \times 2^{16} = 2^{48.74}$ G computations for each plaintext quartet. Moreover, Step 4-(e) is the same procedure as Steps 4-(c) and 4-(d), so Step 4-(e) also requires about $2^{48.74}$ G computations for each plaintext quartet. In Step 4-(f) the expectation of counter for each wrong key is $2^{27.68} \times 2^{32.74} \times 2^{-80} = 2^{-19.58}$. Since the value of the counter behaves like Poisson random variables, we estimate the number of keys in $\mathcal{K}$ using $Poi(2^{-19.58})$. Let the counter value for a wrong key be a variable X, then $X \sim Poi(2^{-19.58})$. Since $Pr[X \geq 2] \approx 1 - (e^{-2^{-19.58}} + e^{-2^{-19.58}} \times (2^{-19.58})) = 2^{-40.16}$, the expected number of $|\mathcal{K}|$ is about $2^{80} \times 2^{-40.16} = 2^{39.84}$ and thus the time complexity of Step 5 is about $2^{38.84}$ 23-round Skipjack encryptions on average. Hence, the overall time complexity of this attack is about $2^{27.68} \times 2 \times 2^{48.74} = 2^{77.42}$ G computations, equivalently $2^{77.42} \times (1/23) = 2^{72.9}$ 23-round Skipjack encryptions, dominated by Steps 4-(d) and 4-(e).

The success rate of this attack is computed as follows: Recall that the last 19-round rectangle distinguisher used in this attack has a probability of 2^{-79} and the first 4-round differential has a probability of $2^{-20.84}$. Since the number of quartets used in this attack is $2^{122.68}$, the expected number of right quartets is $2^{122.68} \times 2^{-79} \times (2^{-20.84})^2 = 4$. This means that the expectation of the counter for the right key is 4. Thus the success rate of this attack is about 90% by $X \sim Poi(4)$, i.e., $Pr[X \geq 2] \approx 0.90$.

Note: In this attack we can use arbitrary nonzero differences c_1, c_3, c_4 instead of $0||52_x$ and $f5_x||0$ (see Eq. (5)). This allows us to use plaintext structures to generate many pairs (and quartets) with a small amount of plaintexts (e.g., a small amount of data complexity). As mentioned before, however, the first 4-round differential used in the attack has a probability less than $2^{-20.84}$, (i.e., about 2^{-32}), so the attack requires much time complexity. We have observed that this attack can be done with a data complexity of 2^{37} chosen plaintexts, a time complexity of $2^{78.48}$ 23-round Skipjack encryptions and a memory complexity of 2^{78} bytes for the same success rate.

Related-Key Rectangle Attacks on 20-Round Skipjack: Similarly, we can construct 16-round related-key rectangle distinguishers with probability 2^{-111}, and use them to show that the related-key rectangle attack can be mounted on Skipjack reduced from 32 to 20 rounds. See Appendix B for more details of the attacks.

Attacks Using the Distinguishers in Corollaries: Similar attacks on other Skipjack variants can also be mounted using the distinguishers presented in Corollaries 2, 3 and 4, requiring similar work and text complexities.

6 Concluding Remarks

We have revisited the structure of Skipjack in terms of its resistance to the more recent advanced differential-style distinguishers that were not considered by its designers nor in previous work on Skipjack. In Table 2, we compare our results with previous attacks on Skipjack variants.

Our related-key attacks (i.e. related-key rectangle and related-key miss-in-the-middle attacks) are better than all the previous related-key attacks on Skipjack.

Further, note that our boomerang-style and related-key attacks apply in symmetry, i.e. if we have an attack on some Skipjack rounds starting with A rounds, a similar attack applies with a corresponding version starting with B rounds (c.f. Table 2).

Table 2 also shows that for Skipjack, related-key attacks are worse than non-related-key ones (e.g., in Differential *vs* RK-Differential, Rectangle *vs* RK-Rectangle, Impossible Differential *vs* RK-MisM and Square *vs* RK-Square). Thus, it counter-intuitively appears that the structure of Skipjack is more resistant to related-key distinguishers than it is to non-related-key ones. Recall that the related-key attack model requires the stronger assumption that an attacker has access to encryption/decryption oracles under the control of two or more unknown keys that are related in some way, thus one would expect it to perform better than non-related-key attacks.

This appears to be due to:

- the high-level structure admits good truncated differentials (used to build the infamous 24-round impossible differential of Skipjack [4]), e.g., the bijectiveness of G allows a zero (respectively non-zero) difference to pass through unchanged (a zero difference remains a zero difference, while a non-zero difference remains non-zero), and zero differences do not affect other differences when combined via XOR.
- the structure complicates the propagation of related-key differentials, e.g., the related-key differentials that we use, exploit the invariance of a non-zero difference past G by depending on the round keys to G having that same difference, thus cancelling out each other. However, the invariant non-zero difference would affect other differences via XOR and thus this limits how far it can propagate unaffected. Also, a zero difference in a related-key differential goes to an arbitrary difference when going past G.

Our results indicate that for the case of Skipjack, related-key attacks are inferior to non-related-key ones. We remark that it does not seem that we can construct related-key impossible differentials longer than the non-related-key one used in [4]. With similar reasoning, related-key differential, square, saturation and rectangle attacks would fare much worse and not get longer distinguishers than non-related-key counterparts.

Table 2. Comparing the Attacks on Skipjack Variants

Attack Variant	Cardinality of Chosen Texts	Round Types	Total Rounds	Texts	Encryptions	Memory	Source
Differential	2	$8r_A \Vert 8r_B$	16	$2^{30.5}$ CP	2^{22}	-	[3]
Differential	2	$8r_A \Vert 8r_B$	16	2^{17} CP	2^{16}	-	[3]
Differential	2	$8r_B \Vert 8r_A$	16	2 CP	2^{51}	-	[44]
Differential	2	$8r_A \Vert 8r_B$	16	2^{17} CP	2^{34}	-	[43]
Differential	2	$8r_B \Vert 8r_A$	16	3 CP	2^{30}	-	[43]
Differential	2	$4r_A \Vert 8r_B \Vert 8r_A \Vert 8r_B{}^{\dagger}$	$28^{\dagger}$	2^{41} CP	2^{77}	-	[43]
Differential	2	$8r_A \Vert 8r_B \Vert 5r_A$	21	2^{17} CP	2^{64}	-	[26]
Differential	2	$8r_A \Vert 8r_B \Vert 8r_A{}^{\dagger\dagger}$	$24^{\dagger\dagger}$	2^{46} CP	2^{72}	-	[26]
Differential	2	$8r_A \Vert 8r_B \Vert 8r_A \Vert 2r_B{}^{\dagger\dagger}$	$26^{\dagger\dagger}$	2^{46} CP	2^{60}	-	[26]
Boomerang	4	$4r_A \Vert 8r_B \Vert 8r_A \Vert 4r_B{}^{\dagger}$	$24^{\dagger}$	2^{25} CP/ACC	2^{25}	-	[43]
Boomerang	4	$5r_A \Vert 8r_B \Vert 8r_A \Vert 4r_B{}^{\dagger}$	$25^{\dagger}$	$2^{34.5}$ CP/ACC	$2^{61.5}$	-	[43]
RK-Differential	2	$4r_A \Vert 8r_B \Vert 2r_A$	14	2^{32} RK-CP	2^{64}	-	[54]
Rectangle	4	$8r_A \Vert 8r_B \Vert 7r_A$	23	$2^{62.84}$ CP	$2^{72.9}$	2^{78}	This paper
Rectangle	4	$7r_B \Vert 8r_A \Vert 8r_B$	23	$2^{62.84}$ CC	$2^{72.9}$	2^{78}	This paper
Rectangle	4	$8r_A \Vert 8r_B \Vert 7r_A$	23	2^{37} CP	$2^{78.48}$	2^{78}	This paper
Rectangle	4	$7r_B \Vert 8r_A \Vert 8r_B$	23	2^{37} CC	$2^{78.48}$	2^{78}	This paper
RK-Rectangle	4	$8r_A \Vert 8r_B \Vert 4r_A$	20	$2^{45.75}$ RK-CP	$2^{78.68}$	2^{78}	This paper
RK-Rectangle	4	$4r_B \Vert 8r_A \Vert 8r_B$	20	$2^{45.75}$ RK-CC	$2^{78.68}$	2^{78}	This paper
Impossible Differential	2	$4r_A \Vert 8r_B \Vert 8r_A \Vert 5r_A$	25	2^{38} CP	2^{27}	2^{16}	[4]
Impossible Differential	2	$5r_A \Vert 8r_B \Vert 8r_A \Vert 5r_A$	26	2^{38} CP	2^{49}	2^{16}	[4]
Impossible Differential	2	$8r_A \Vert 8r_B \Vert 8r_A \Vert 7r_A$	31	2^{41} CP	2^{78}	2^{64}	[4]
Impossible Differential	2	$7r_A \Vert 8r_B \Vert 8r_A \Vert 8r_A$	31	2^{34} CP	2^{78}	2^{64}	[4]
RK-MisM	2	$5r_A \Vert 8r_B \Vert 8r_A \Vert 1r_B$	22	2^{53} RK-CP	$2^{65.12}$	2^{45}	This paper
RK-MisM	2	$1r_A \Vert 8r_B \Vert 8r_A \Vert 5r_B$	22	2^{53} RK-CC	$2^{65.12}$	2^{45}	This paper
Saturation	2^{16}	$4r_A \Vert 8r_B \Vert 6r_A$	18	2^{17} CP	2^{44}	-	[27]
Saturation	2^{16}	$4r_A \Vert 8r_B \Vert 8r_A \Vert 3r_B$	23	2^{18} CP	2^{77}	-	[27]
Saturation	2^{16}	$8r_A \Vert 8r_B \Vert 6r_A$	22	2^{49} CP	2^{44}	-	[27]
Saturation	2^{16}	$8r_A \Vert 8r_B \Vert 8r_A \Vert 3r_B$	27	2^{50} CP	2^{77}	-	[27]
Square	2^{16}	$8r_A \Vert 8r_B$	16	2^{18} CP	2^{76}	-	[55]
Square	2^{16}	$8r_A \Vert 8r_B \Vert 3r_A$	19	2^{18} CP	2^{59}	-	[55]
Square	2^{16}	$8r_A \Vert 8r_B \Vert 7r_A$	23	2^{18} CP	2^{76}	-	[55]
Square	2^{16}	$3r_A \Vert 8r_B \Vert 7r_A$	18	2^{18} CP	2^{43}	-	[55]
Square	2^{16}	$6r_A \Vert 8r_B \Vert 7r_A$	21	2^{18} CP	2^{43}	-	[55]
RK-Square	2^{8}	$8r_A \Vert 1r_B$	9	2^{18} RK-CP	2^{43}	-	[55]
RK-Square	2^{16}	$8r_A \Vert 4r_B$	12	2^{18} RK-CP	2^{44}	-	[55]

†: as pointed out in [24], the attacks do not work.

††: as pointed out in this paper, the attacks do not work.

We emphasize that this does not imply that Skipjack has a very strong key schedule. In fact, it is due to the key schedule that the 24-round impossible differential in [4] could be applied to attack 31 rounds of Skipjack, a major feat indeed.

Instead, our above reasonings imply that the overall diffusion structure of Skipjack is quite weak, and design choices give rise to subtle weaknesses, e.g. a non-bijective G would not have allowed a zero (respectively non-zero) to propagate through it unchanged. The "pluses" for the Skipjack structure appear to be the round counters (that complicate key-schedule attacks) and the use of different round types (A, B).

This work is hoped to shed further light into the NSA design principles of Skipjack, and its security. We leave as open problems if better types of related-key differentials can be found for Skipjack that use differences unlike the type we have used, and how to naturally extend existing related-key differential attacks on other block ciphers e.g. [33, 34], via the RK-MisM technique into related-key impossible differential attacks that cover more rounds.

About the Authors

Jongsung Kim obtained his Bachelor and Master degrees in mathematics from Korea university, Korea in 2000 and 2002, respectively. He received double Doctoral degrees on "Combined Differential, Linear and Related-Key Attacks on Block Ciphers and MAC Algorithms", completed in November 2006 and February 2007 at the ESAT/COSIC group of Katholieke Universiteit Leuven and at Engineering in Information Security of Korea University, respectively. Currently, he is a research professor of Center for Information Security Technologies (CIST) at Korea University. His research interests include symmetric crytosystems, hash functions, MACs, side-channel attacks and ubiquitous computing systems. He serves in technical Program Committees of ISH '05, ISA '09, UASS '09, SSDU '09 and SMPE '09.

Raphael Phan obtained his B. Eng (Hons) Electronics major in Computer Engineering; M. EngSc. (Research) on "Cryptanalysis of the Advanced Encryption Standard (AES) and Skipjack" sponsored by the Intel Fellowship Grant award; and Ph.D (Eng) on "Cryptanalysis of Block Ciphers: Generalization, Extensions & Integrations", from Multimedia University (MMU). Prior to joining the Electronic and Electrical Engineering department of Loughborough University, UK, Raphael was Director of the Information Security Research (iSECURES) Laboratory at Swinburne Uni of Tech from 2004 to 2007; and a researcher in the Laboratoire de sécurité et de cryptographie (LASEC), Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland between 2007 and 2008. He researches on the security of ciphers, protocols; and related constructions. He is General Chair of Mycrypt '05 and Asiacrypt '07, Program Chair of ISH '05, and serves in technical Program Committees of international conferences since 2005.

Acknowledgements

We thank the referees for constructive comments and interest in this work. We thank God for His many blessings (Dt 8:13).

References

1. Biham, E., "New Types of Cryptanalytic Attacks Using Related Keys", Advances in Cryptology – Eurocrypt '93, Lecture Notes in Computer Science, vol. 765, pp. 398-409, Springer-Verlag, 1994.
2. Biham, E., "New Types of Cryptanalytic Attacks Using Related Keys", Journal of Cryptology, vol. 7, pp. 229–246, 1994.
3. Biham, E., A. Biryukov, O. Dunkelman, E. Richardson and A. Shamir, "Initial Observations on Skipjack – Cryptanalysis of Skipjack-3XOR", SAC '98, Lecture Notes in Computer Science, vol. 1556, pp. 362-370, Springer-Verlag, 1998.
4. Biham, E., A. Biryukov and A. Shamir, "Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials", Advances in Cryptology – Eurocrypt '99, Lecture Notes in Computer Science, vol. 1592, pp. 12-23, Springer-Verlag, 1999.
5. Biham, E., A. Biryukov and A. Shamir, "Miss in the Middle Attacks on IDEA, Khufu and Khafre", FSE '99, Lecture Notes in Computer Science, vol. 1636, pp. 124-138, Springer-Verlag, 1999.
6. Biham, E., O. Dunkelman and N. Keller, "The Rectangle Attack – Rectangling the Serpent", Advances in Cryptology – Eurocrypt '01, Lecture Notes in Computer Science, vol. 2045, pp. 340-357, Springer-Verlag, 2001.
7. Biham, E., O. Dunkelman and N. Keller, "New Results on Boomerang and Rectangle Attacks", FSE '02, Lecture Notes in Computer Science, vol. 2365, pp. 1-16, Springer-Verlag, 2002.
8. Biham, E., O. Dunkelman and N. Keller, "Rectangle Attacks on 49-Round SHACAL-1", FSE '03, Lecture Notes in Computer Science, vol. 2887, pp. 22-35, Springer-Verlag, 2003.
9. Biham, E., O. Dunkelman and N. Keller, "Related-Key Boomerang and Rectangle Attacks", Advances in Cryptology – Eurocrypt '05, Lecture Notes in Computer Science, vol. 3494, pp. 507-525, Springer-Verlag, 2005.
10. Biham, E., O. Dunkelman and N. Keller, "A Related-Key Rectangle Attack on the Full KASUMI", Advances in Cryptology – Asiacrypt '05, Lecture Notes in Computer Science, vol. 3788, pp. 443-461, Springer-Verlag, 2005.
11. Biham, E., O. Dunkelman and N. Keller, "Related-Key Impossible Differential Attacks on 8-Round AES-192", Topics in Cryptology – CT-RSA '06, Lecture Notes in Computer Science, vol. 3860, pp. 21-33, Springer-Verlag, 2006.
12. Biham, E. and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems (Extended Abstract)", Advances in Cryptology – Crypto '90, Lecture Notes in Computer Science, vol. 537, pp. 2-21, Springer-Verlag, 1991.
13. Biham, E. and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Journal of Cryptology, vol. 4, no. 1, pp. 3–72, 1991.
14. Biryukov, A., "Methods of Cryptanalysis", Ph.D. Dissertation, Technion, Israel, 1999.

15. Biryukov, A., "The Boomerang Attack on 5 and 6-round Reduced AES", AES4, Lecture Notes in Computer Science, vol. 3373, pp. 1-5, Springer-Verlag, 2004.
16. Biryukov, A., C. De Canniere and G. Dellkrantz, "Cryptanalysis of SAFER++", Advances in Cryptology – Crypto '03, Lecture Notes in Computer Science, vol. 2729, pp. 195-211, Springer-Verlag, 2003.
17. Biryukov, A., J. Nakahara Jr, B. Preneel and J. Vandewalle, "New Weak-Key Classes of IDEA", ICICS '02, Lecture Notes in Computer Science, vol. 2513, pp. 315-326, Springer-Verlag, 2002.
18. Biryukov, A. and D. Wagner, "Slide Attacks", FSE '99, Lecture Notes in Computer Science, vol. 1636, pp. 245–259, Springer-Verlag, 1999.
19. Biryukov, A. and D. Wagner, "Advanced Slide Attacks", Advances in Cryptology – Eurocrypt '00, Lecture Notes in Computer Science, vol. 1807, pp. 589–606, Springer-Verlag, 2000.
20. Brickell, E.F., D.E. Denning, S.T. Kent, D.P. Maher and W. Tuchman, "SKIPJACK Review: The SKIPJACK Algorithm", Interim Report, July 28, 1993.
21. Diffie, W. and S. Landau, "Privacy on the Line", MIT Press, 1998.
22. Dunkelman, O., N. Keller, J. Kim, "Related-Key Rectangle Attack on the Full SHACAL-1", SAC '06, Lecture Notes in Computer Science, vol. 4356, pp. 28-44, Springer-Verlag, 2006.
23. Gorski, M. and S. Lucks, "New Related-Key Boomerang Attacks on AES", Progress in Cryptology - Indocrypt '08, Lecture Notes in Computer Science, vol. 5365, pp. 266-278, Springer-Verlag, 2008.
24. Granboulan, L., "Flaws in the Differential Cryptanalysis of Skipjack", FSE '01, Lecture Notes in Computer Science, vol. 2355, pp. 328–335, Springer-Verlag, 2001.
25. Hong, S., J. Kim, G. Kim, S. Lee and B. Preneel, "Related-key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192", FSE '05, Lecture Notes in Computer Science, vol. 3557, pp. 368-383, Springer-Verlag, 2005.
26. Hui, L.C.K., X.Y. Wang, K.P. Chow, W.W.Tsang, C.F.Chong and H.W. Chan, "The Differential Analysis of Reduced Skipjack Variants", Chinacrypt '02, 2002.
27. Hwang, K., W. Lee, S. Lee, S. Lee and J. Lim, "Saturation Attacks on Reduced Round Skipjack", FSE '02, Lecture Notes in Computer Science, vol. 2365, pp. 100-111, Springer-Verlag, 2002.
28. Jakimoski, G. and Y. Desmedt, "Related-key Differential Cryptanalysis of 192-bit Key AES Variants", SAC '03, Lecture Notes in Computer Science, vol. 3006, pp. 208–221, Springer-Verlag, 2003.
29. Jeong, K., C. Lee, J. Sung, S. Hong and J. Lim, "Related-key Amplified Boomerang Attacks on the Full-Round Eagle-64 and Eagle-128", ACISP '07, Lecture Notes in Computer Science, vol. 4586, pp. 143-157, Springer-Verlag, 2007.
30. Joux, A. and T. Peyrin, "Hash Functions and the Boomerang Attack", ECRYPT Hash Workshop, May 2007.
31. Joux, A. and T. Peyrin, "Hash Functions and the (Amplified) Boomerang Attack", Advances in Cryptology – Crypto '07, Lecture Notes in Computer Science, vol. 4622, pp. 244–263, Springer-Verlag, 2007.
32. Kelsey, J., T. Kohno and B. Schneier, "Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent", FSE '00, Lecture Notes in Computer Science, vol. 1978, pp. 75-93, Springer-Verlag, 2000.
33. Kelsey, J., B. Schneier and D. Wagner, "Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES", Advances in Cryptology – Crypto '96, Lecture Notes in Computer Science, vol. 1109, pp. 237–251, Springer-Verlag, 1996.
34. Kelsey, J., B. Schneier and D. Wagner, "Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2 and TEA", ICICS '97, Lecture Notes in Computer Science, vol. 1334, pp. 233–246, Springer-Verlag, 1997.
35. Kim, J., S. Hong and B. Preneel, "Related-Key Rectangle Attacks on Reduced AES-192 and AES-256", FSE '07, Lecture Notes in Computer Science, vol. 4593, pp. 225–241, Springer-Verlag, 2007.
36. Kim, J., G. Kim, S. Hong, S. Lee and D. Hong, "The Related-key Rectangle Attacks – Application to SHACAL-1", ACISP '04, Lecture Notes in Computer Science, vol. 3108, pp. 123-136, Springer-Verlag, 2004.
37. Kim, T., J. Kim, S. Hong and J. Sung, "Linear and Differential Cryptanalysis of Reduced SMS4 Block Cipher", IACR ePrint Archive, 2008/281, 2008.
38. Kim, J., G. Kim, S. Lee, J. Lim and J. Song, "Related-Key Attacks on Reduced-Rounds of SHACAL-2", Progress in Cryptology - Indocrypt '04, Lecture Notes in Computer Science, vol. 3348, pp. 175-190, Springer-Verlag, 2004.
39. Kim, J., D. Moon, W. Lee, S. Hong, S. Lee and S. Jung, "Amplified Boomerang Attacks Against Reduced-Round SHACAL", Advances in Cryptology – Asiacrypt '02, Lecture Notes in Computer Science, vol. 2501, pp. 243-253, Springer-Verlag, 2002.
40. Knudsen, L.R., "Block Ciphers - Analysis, Design and Applications", Aarhus University, Ph.D. Dissertation, DAIMI PB-485, 1994.
41. Knudsen, L.R., "Truncated and Higher Order Differentials", FSE '94, Lecture Notes in Computer Science, vol. 1008, pp. 196-211, Springer-Verlag, 1995.
42. Knudsen, L.R., "DEAL - a 128-bit Block Cipher", Technical Report 151, Department of Informatics, University of Bergen, Norway, February 1998. Submitted as an AES candidate.

43. Knudsen, L.R., M.J.B. Robshaw and D. Wagner, "Truncated Differentials and Skipjack", Advances in Cryptology – Crypto '99, Lecture Notes in Computer Science, vol. 1666, pp. 163-180, Springer-Verlag, 1999.
44. Knudsen, L.R. and D. Wagner, "On the Structure of Skipjack", Discrete Applied Mathematics, vol. 111, pp. 103–116, 2001.
45. Koho, T., "Requirement for Conventional Differentials in Amplified Boomerangs", private communication, 2000.
46. Lee, E., J. Kim, D. Hong, C. Lee, J. Sung, S. Hong and J. Lim, "Weak-Key Classes of 7-Round MISTY 1 and 2 for Related-Key Amplified Boomerang Attacks", IEICE Transactions, vol. 91-A(2), pp. 642–649, 2008.
47. Lee, C., J. Kim, S. Hong, J. Sung and S. Lee, "Security Analysis of the Full-Round DDO-64 Block Cipher", Journal of Systems and Software, vol. 81(1), pp. 2328–2335, 2008.
48. Lu, J., "Attacking Reduced-Round Versions of the SMS4 Block Cipher in the Chinese WAPI Standard", ICICS '07, Lecture Notes in Computer Science, vol. 4861, pp. 306-318, Springer-Verlag, 2007.
49. Lu, J., "Related-Key Rectangle Attack on 36 Rounds of the XTEA Block Cipher", International Journal of Information Security, in press, online first July 2008.
50. Lu, J. and J. Kim, "Attacking 44 Rounds of the SHACAL-2 Block Cipher using Related-Key Rectangle Cryptanalysis", IEICE Transactions, vol. 91-A(9), pp. 2588–2596, 2008.
51. Lu, J., J. Kim, N. Keller and O. Dunkelman, "Related-Key Rectangle Attack on 42-Round SHACAL-2", ISC '06, Lecture Notes in Computer Science, vol. 4176, pp. 85-100, Springer-Verlag, 2006.
52. Lu, J., J. Kim, N. Keller and O. Dunkelman, "Differential and Related-Key Rectangle Attacks on Reduced-Round SHACAL-1", Progress in Cryptology - Indocrypt '06, Lecture Notes in Computer Science, vol. 4329, pp. 17-31, Springer-Verlag, 2006.
53. Lu, J., C. Lee, J. Kim, "Related-Key Attacks on the Full-Round Cobra-F64a and Cobra-F64b", SCN '06, Lecture Notes in Computer Science, vol. 4116, pp. 95-110, Springer-Verlag, 2006.
54. Lucks, S. and R. Weis, "A Related-key Attack against 14 Rounds of Skipjack", Technical Report, Universitat Mannheim, 1999.
55. Nakahara, J., Jr., B. Preneel and J. Vandewalle, "Square Attacks on Reduced-Round Variants of the Skipjack Block Cipher", IACR ePrint Archive, 2002/003, 2002.
56. National Institute of Standards and Technology (NIST), "Skipjack and KEA Algorithm Specifications. Version 2", 1998.
57. Phan, R.C.-W., "Cryptanalysis of the Advanced Encryption Standard (AES) & Skipjack", M.Eng.Sc. Thesis, Multimedia University, May 2001.
58. Phan, R.C.-W., "Related-key Impossible Differential Cryptanalysis of Skipjack", unpublished manuscript, submitted 2002.
59. Phan, R.C.-W. and A. Shamir, "Improved Related-Key Attacks on DESX and DESX+", Cryptologia, vol. 32(1), pp. 13–22, 2008.
60. Pierce, G. and C. Paar, "Recent Developments in Digital Wireless Network Security", Technical Conference on Telecommunications Research and Development in Massachusetts, Lowell, March 12, 1996.
61. Reichardt, B. and D. Wagner, "Markov Truncated Differential Cryptanalysis of Skijjack", SAC '02, Lecture Notes in Computer Science, vol. 2595, pp. 110-128, Springer-Verlag, 2002.
62. Schneier, B. and D. Banisar, "The Electronic Privacy Papers", John Wiley & Sons, 1997.
63. Wagner, D., "The Boomerang Attack", FSE '99, Lecture Notes in Computer Science, vol. 1636, pp. 156-170, Springer-Verlag, 1999.
64. G. Wang, "Related-Key Rectangle Attack on 43-Round SHACAL-2", ISPEC '07, Lecture Notes in Computer Science, vol. 4464, pp. 33-42, Springer-Verlag, 2007.

A Schematic Descriptions of Complementation Properties and Round Functions of Skipjack

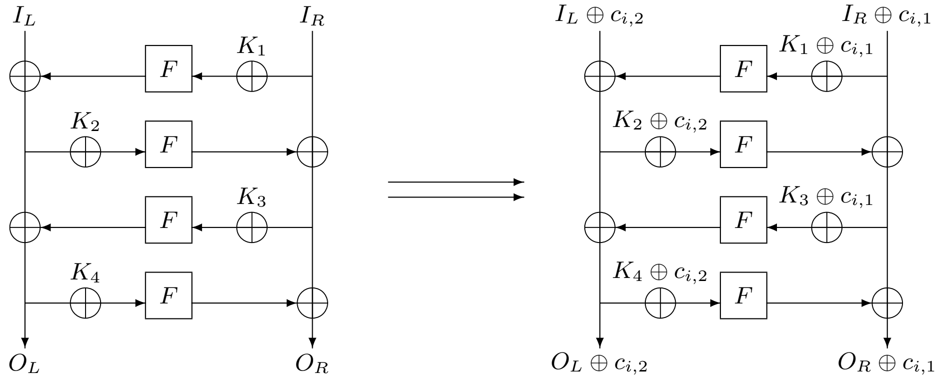
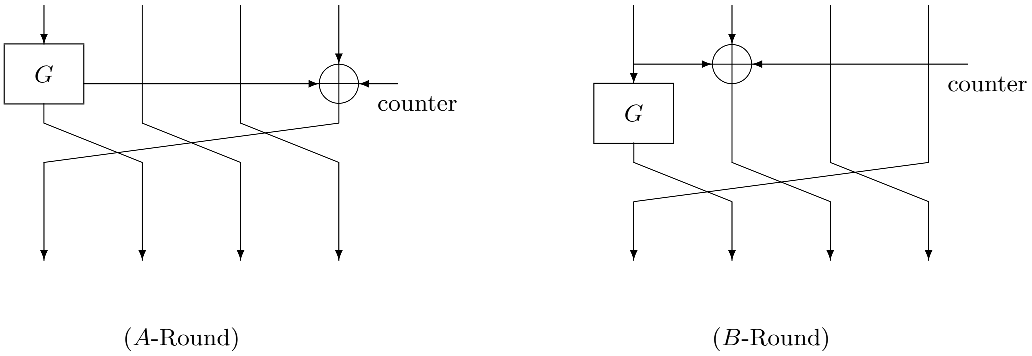


Fig. 1. Complementation Properties of the G Permutation



(A-Round)

(B-Round)

Fig. 2. Round Functions of Skipjack

B Related-Key Rectangle Attacks on 20-Round Skipjack

It is intuitive to consider recent related-key rectangle attacks [36, 25, 9, 10] for Skipjack, since it has a simple key schedule allowing much control over round key differences.

Theorem 4: There exists a 16-round related-key rectangle distinguisher through $4r_A||8r_B||4r_A$ of the form $\{\alpha, \delta\} = \{(0, c_1, 0, 0), (0, \overline{a}, \overline{a}, \overline{a})\}$ with probability 2^{-111}, where c_1 is an arbitrary nonzero difference and $\Delta K = (a, a, a, a, a)$.

Proof of Theorem 4: Let $E_0 = 4r_A||8r_B$ and $E_1 = 4r_A$. Use a 12-round probability-one truncated differential $\{\alpha, \beta\} = \{(0, c_1, 0, 0), (c_2, c_3, c_4, 0)\}$ to cover E_0, and 4-round probability-one related-key truncated differential $\{\gamma, \delta\} = \{(\overline{a}, 0, 0, 0), (0, \overline{a}, \overline{a}, \overline{a})\}$ to cover E_1, under two related keys (K, K') with difference $\Delta K = (a, a, a, a, a)$. This can be used to form a Type 2 related-key rectangle distinguisher [36]. When we have $\{\alpha, \beta\} = \{(0, c_1, 0, 0), (c_2, c_3, c_4, 0)\}$ going through both E_0 with probability one, we then get with probability 2^{-64} that $E_0(P_1) \oplus E_0(P_3) = \gamma = (\overline{a}, 0, 0, 0)$, and thus the boomerang condition in the middle, i.e. $E_0(P_2) \oplus E_0(P_4) = \gamma = (\overline{a}, 0, 0, 0)$, will be satisfied with probability 2^{-48}. This allows for $\{\gamma, \delta\} = \{(\overline{a}, 0, 0, 0), (0, \overline{a}, \overline{a}, \overline{a})\}$ to go through the both E_1 with probability one. Furthermore, it can be also applied to (P_1, P_4) and (P_2, P_3). The resultant probability is thus $2 \times 2^{-64} \times 2^{-48} = 2^{-111}$, compared to the probability of 2^{-127} that it would occur for a random permutation. □

Similarly, there is another 16-round related-key rectangle distinguisher through the 16 rounds $4r_B^{-1}||8r_A^{-1}||4r_B^{-1}$.

Corollary 4: There exists a 16-round related-key rectangle distinguisher through $4r_B^{-1}||8r_A^{-1}||4r_B^{-1}$ of the form $\{\alpha, \delta\} = \{(c_1, 0, 0, 0), (\overline{a}, 0, \overline{a}, \overline{a})\}$ with probability 2^{-111}, where c_1 is an arbitrary nonzero difference and $\Delta K = (a, a, a, a, a)$.

B.1 The Attacks

We amount a related-key rectangle attack on Skipjack reduced to 20 rounds, from the 1-st round to the 20-th round, namely $8r_A||8r_B||4r_A$. We apply the 16-round related-key rectangle distinguisher in Theorem 4 to the last 16 rounds, and retrieve keys in the first 4 rounds.

This attack is very similar to the previous rectangle attack. The 16-round related-key rectangle distinguisher has a probability of 2^{-111}, which is much less than that of the 19-round rectangle distinguisher in Theorem 3. The probability 2^{-111} does not allow us to use $c_1 = 0||52_x$ and $c_3 = c_4 = f5_x||0$ in Eq. (5) (because if we use them in our attack, we cannot generate the amount of required quartets even though we use all possible plaintexts). So we should use in Eq. (5) arbitrary nonzero differences c_1, c_3 and c_4. It follows that the first 4-round differential used in the attack has a probability of 2^{-32}, and thus the overall probability of 20 rounds is $2^{-111} \times (2^{-32})^2 = 2^{-175}$. In order to get 4 right quartets, the number of required quartets in the attack should be 2^{177}. To collect these required quartets, we choose $2^{44.75}$ plaintexts whose third 16-bit values are all same under key K as well as choose the same amount of plaintexts whose third 16-bit values are also same under key $K \oplus \Delta K$. These form $(\frac{(2^{44.75})^2}{2})^2 = 2^{177}$ quartets. Moreover, the number of quartets tested in Step 4 of the previous attack algorithm is 2^{50} because the filtering condition of Step 2 comprises 127 bits.

As stated earlier, differential $c_4 \xrightarrow{G} c_1$ in round 1 holds with probability 2^{-16}. It follows that in Step 4-(a) the expectation of $|\mathcal{L}1|$ is one, and this step requires $2^{50} \times 2^{17} = 2^{67}$ G computations in all. Similarly, differential $c_3 \xrightarrow{G} c_1$ in round 4 also holds with probability 2^{-16}, so in Step 4-(b) the expectation of $|\mathcal{L}2|$ is 2^{16}(but it covers 2^{32}) and this step requires $2^{50} \times 2^{16} = 2^{66}$ G computations in all. Thus the expectations of $|\mathcal{L}3|$ and $|\mathcal{L}4|$ are one(but it covers 2^{16}) and 2^{32}, respectively. From the previous analysis, we see that Step 4-(d) and Step 4-(e) require $2^{50} \times 2 \times 2^{32} = 2^{83}$ G computations in all. Since the expectation of $|\mathcal{K}|$ is $2^{16} \times (2^{16})^2 \times 2^{-32} = 2^{16}$, the expected counter for each wrong key is about $2^{50} \times 2^{16} \times 2^{-80} = 2^{-14}$, which is almost the same as the previous one. It means that the time complexity of Step 5 is much less than Step 4.

Hence, this attack can be done with a data complexity of $2^{45.75}$ related-key chosen plaintexts, a time complexity of $2^{83} \times (1/20) = 2^{78.68}$ 20-round Skipjack encryptions and a memory complexity of 2^{78} bytes for the same success rate 90%.

C Boomerang-Style Attacks on Block Ciphers

For a better appreciation, we chronologically list boomerang-style attacks in literature, and corresponding ciphers on which they were applied.

Boomerang

1. Wagner [63], 1999: COCONUT98, Khufu-16, FEAL-6, CAST-256.

2. Biham et al. [7], 2002: SC2000, Serpent.
3. Biryukov et al. [17], 2002: IDEA.
4. Biryukov et al. [16], 2003: SAFER++.
5. Biryukov [15], 2004: AES-128.
6. Biham et al. [9], 2005: COCONUT98, IDEA.
7. Kim et al. [37], 2008: SMS4.

Amplified Boomerang

1. Kelsey et al. [32], 2000: Serpent, MARS.
2. Kim et al. [39], 2002: SHACAL-1.

Rectangled Amplified Boomerang

1. Biham et al. [6], 2001: Serpent.
2. Biham et al. [7], 2002: SC2000, Serpent.
3. Biham et al. [8], 2003: SHACAL.
4. Lu et al. [52], 2006: SHACAL-1.
5. Lu [48], 2007: SMS4.
6. Kim et al. [37], 2008: SMS4.
7. This paper, 2009: Skipjack.

Related-Key Variants

1. Kim et al. [36] (Rectangle), 2004: SHACAL-1.
2. Kim et al. [38] (Rectangle), 2004: SHACAL-2.
3. Hong et al. [25] (Rectangle), 2005: SHACAL-1, AES-192.
4. Biham et al. [9] (Boomerang & Rectangle), 2005: AES-192, AES-256, COCONUT98, IDEA.
5. Biham et al. [10] (Rectangle), 2005: KASUMI.
6. Dunkelman et al. [22] (Rectangle), 2006: SHACAL-1.
7. Lu et al. [51] (Rectangle), 2006: SHACAL-2.
8. Lu et al. [53] (Rectangle), 2006: Cobra-F64a, Cobra-F64b.
9. Kim et al. [35] (Rectangle), 2007: AES-192, AES-256.
10. Jeong et al. [29] (Amplified Boomerang), 2007: Eagle-64, Eagle-128.
11. Wang [64] (Rectangle), 2007: SHACAL-2.
12. Lee et al. [46] (Amplified Boomerang), 2008: MISTY1, MISTY2.
13. Lee et al. [47] (Boomerang, Amplified Boomerang), 2008: DDO-64.
14. Lu and Kim [50] (Rectangle), 2008: SHACAL-2.
15. Gorski and Lucks [23] (Boomerang), 2008: AES.
16. This paper (Rectangle), 2009: Skipjack.