A Study of Partial Non-Linear Layers with DEFAULT and BAKSHEESH

Anubhab Baksi

Nanyang Technological University, Singapore

anubhab.baksi@ntu.edu.sg

Abstract. In this work, we take a look at the two recently proposed block ciphers, DEFAULT and BAKSHEESH, both of which are descendent of another block cipher named GIFT. We show that both ciphers can be interpreted within the partial non-linear layer category, thanks to the SBoxes having at least one non-trivial linear structure. We also reevaluate the security claim of DEFAULT.

Keywords: SBox · Linear Structure · Partial Non-Linear Layer · GIFT · DEFAULT · BAKSHEESH

1 Introduction

Over the course of cipher design in the realm of symmetric-key cryptography, a few genres have emerged. Relatively recently, the so-called lightweight ciphers are dominating the research landscape. This is reflected from a plenitude of mainstream ciphers, arguably starting with PRESENT [9], thereafter followed by popular ciphers like SKINNY [7] or GIFT [6]. Recently, we have seen a new cipher named BAKSHEESH [4] which continues the legacy of GIFT (also borrowing idea from DEFAULT [2] in the process). In the design of BAKSHEESH, an unorthodox SBox is chosen, in which the one of the coordinate functions of the constituent SBox is affine.

Contribution

We choose the following representative ciphers:

- **DEFAULT.** DEFAULT [2] is designed to have non-trivial security against *Differential Fault Attack* (DFA) [3] by virtue of design (i.e., not relying on any additional implementation/protocol level countermeasure). DEFAULT does not directly use a partially non-linear layer (in the same sense as ZORRO [10] does), as the SBoxes cover the entire state (thirty two 4-bit SBoxes for 128-bit state). However, two (out of four) coordinate functions of the SBox are affine, making the substitution layer equivalent to half affine and half constituted of thirty two 2-bit SBoxes. However, DEFAULT does not deliver its promise, as we discuss here.
- **BAKSHEESH.** Unlike the niche-specific ciphers, BAKSHEESH [4] brings the concept of partial non-linear layer to the mainstream. Similar to DEFAULT, one coordinate function of its thirty two SBoxes is affine, thereby making the substitution layer of the cipher having only a ninety six bit non-linear layer. BAKSHEESH takes less number of rounds compared to its predecessor GIFT-128 and offers an edge due to its low AND count/depth.

This project is partially supported by the Wallenberg – NTU Presidential Post-doctoral Fellowship.

2 Background

Conversion of elements between $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ is considered intrinsically. In the following, $\cdot$ denotes the dot product. With respect to an $n \times n$ SBox S, the following $2^n \times 2^n$ matrices (typically termed as tables) are proposed/used in the literature:

- *Difference Distribution Table* (DDT): $\mathrm{DDT}[\delta, \Delta] = |\{x \in \mathbb{F}_2^n \ni S(x) \oplus S(x \oplus \delta) = \Delta\}|$.
- *Linear Approximation Table* (LAT): $\mathrm{LAT}[\gamma, \Gamma] = |\{x \in \mathbb{F}_2^n \ni \gamma \cdot x = \Gamma \cdot S(x)\}| - 2^{n-1}$.
- *Boomerang Connectivity Table* (BCT): $\mathrm{BCT}[\phi, \Phi] = |\{x \in \mathbb{F}_2^n \ni S^{-1}(S(x) \oplus \Phi) \oplus S^{-1}(S(x \oplus \phi) \oplus \Phi) = \phi\}|$.
- *Autocorrelation Table* (ACT): $\mathrm{ACT}[\psi, \Psi] = |\{x \in \mathbb{F}_2^n \ni \Psi \cdot S(x) = \Psi \cdot S(x \oplus \psi)\}| - |\{x \in \mathbb{F}_2^n \ni \Psi \cdot S(x) \neq \Psi \cdot S(x \oplus \psi)\}|$.

Definition 1 (Linear Structure (LS)). *The element λ is called a linear structure (LS) of S, if $S(x) \oplus S(x \oplus \lambda)$ is a constant $\forall x$.*

Definition 2 (Differential/Linear Branch Number). *The Differential Branch Number (DBN) is defined as $\min_{\delta \neq 0}\{\mathrm{HW}(\delta) + \mathrm{HW}(S(x) \oplus S(x \oplus \delta))\}$; and that of the Linear Branch Number (LBN) as $\min\{\mathrm{HW}(\gamma) + \mathrm{HW}(\Gamma)\}$ given $\gamma \neq 0, \mathrm{LAT}[\gamma, \Gamma] \neq 0$; where $\mathrm{HW}(\cdot)$ denotes the Hamming weight.*

Definition 3 (Coordinate Function and Component Function). *Suppose $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is defined as $F(x) = (f_0(x), \ldots, f_{n-1}(x))$ for all $x \in \mathbb{F}_2^n$, where $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$ for $i = 0, \ldots, n-1$. Then each f_i is called a coordinate function of F. The linear combinations of f_i's are called the component functions of F.*

Definition 4 (Non-linearity). *The non-linearity of the Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is the minimum Hamming distance of f to the set of all affine functions. Further, the non-linearity of $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is the minimum of the non-linearity of all the component functions of F.*

Note that, $\mathrm{DDT}[0, 0]$ is the maximum, i.e., 2^n, and the rest of the elements in this row and column are all 0; and 0 is the trivial LS. The maximum entry in the DDT except $\mathrm{DDT}[0, 0]$ is known as the *Differential Uniformity* (DU). Similarly, the maximum entry in the BCT except $\mathrm{BCT}[0, 0]$ is called the *Boomerang Uniformity* (DU). Note that, LS implies the DU is 2^n. Further, the number of LS equals the frequency of DU in the DDT. The concept of the linear structure (Definition 1) can be described with *Boolean derivative* (the derivative is constant at LS).

3 Specific Research & Development Domains

3.1 Sandwich Construction

The *sandwich construction* was originally proposed in `DEFAULT` [2]. The basic idea of this construction is to have two unkeyed permutations (called, *layer*) with some properties to sandwich another unkeyed permutation (called, *core*); wherein the core and the layers have opposing properties. In case of `DEFAULT`, the layers are supposed to provide security against DFA, at the expense of being comparatively vulnerable against the classical attacks. The core, on the other hand, is relatively stronger than the layer in terms of the classical attacks, but does not have any discernible security against DFA.

3.2 DEFAULT

As noted already, DEFAULT [1] is the first cipher to have an in-built DFA security claim. Fault countermeasures designed prior to the introduction of DEFAULT rely on some assumption beyond the reach/control for the cipher designer. This compartmentalised approach makes the overall solution esoteric to the device implementer or network administrator (since it can not be interpreted/ensured at the cipher design level), not to mention hampering all-round analysis and development.

Unfortunately, DEFAULT falls short of its promise. The usage of LS SBox in a cipher construction, while novel by its merit, introduces some other weakness that can be exploited in DFA. One may observe that two (out of four) bits of the SBox involve in non-linear operation, while the rest two pass as an affine function at a given round. Half of the state bits which are not involved in a non-linear operation, can be considered to diffuse with the rest half (which involve non-linear operation) by a linear layer which applies state-wise. One half of the state bits at given round is first updated by a 2 × 2 SBox, while the rest half remain as-is. Then the whole state enters a linear layer (which is no longer a bit-permutation, but contains XOR operations). Figure 1 shows the simplified schematic for the difference transition when the SBox is considered as a whole and 2 coordinate functions are affine.

It is evident that it is not possible to recover individual round keys if those are XORed. However, the attacker does not have to recover the round keys. In this case though, the attacker will actually recover the equivalent keys (instead of the actual round key), which are linear operations of the round keys due to the two affine coordinate functions of the SBox. The equivalent round keys are formed as some of the bits of round keys from the previous round will be associated with the target (for DFA) round in an affine way.

This idea still works even when the round keys are independent has no bearing (in other words, the attacker is able to do virtually the same analysis even if the round keys are independent).

Note that DEFAULT does not claim any security against faults that simultaneously target encryption and decryption (cf., the corresponding analysis in [11]).

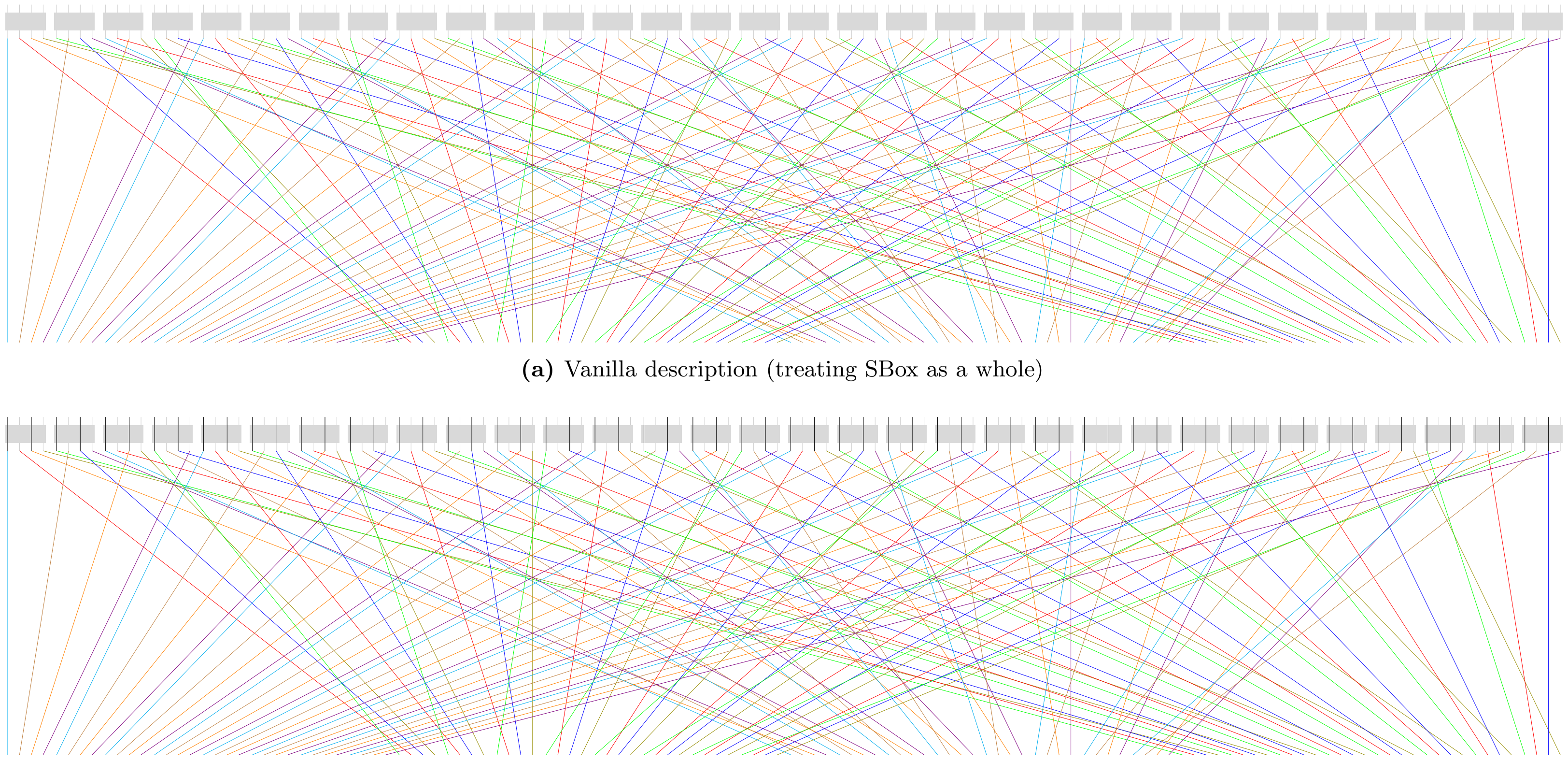
3.3 BAKSHEESH

One may note that the classical security of DEFAULT-LAYER (if it is considered as a standalone cipher) takes about 80 rounds (i.e., comparble to duplicated GIFT-128). As the SBox contains 4 non-trivial LS, one could expect that having 2 non-trivial LS would make it comparable to GIFT-128. The main advantage will be that low AND count/depth. SCA (as the SBox has only affine and quadratic coordinate functions) 3-share TI [5,8] would suffice.

Such SBox was, more than likely, not considered during the design of GIFT. LS to design mainstream cipher can be considered end-of-line, it does not seem possible to introduce new innovation into the mainstream (lightweight) cipher construction.

From an alternate but equivalent description (analogous to DEFAULT-LAYER, as described in Section 3.2), BAKSHEESH can be described to have a partial non-linear layer, thanks to its usage of an SBox with LS. Thus, in some sense, it bridges the gap between mainstream ciphers (like, PRESENT or GIFT) with the nice-specific ciphers.

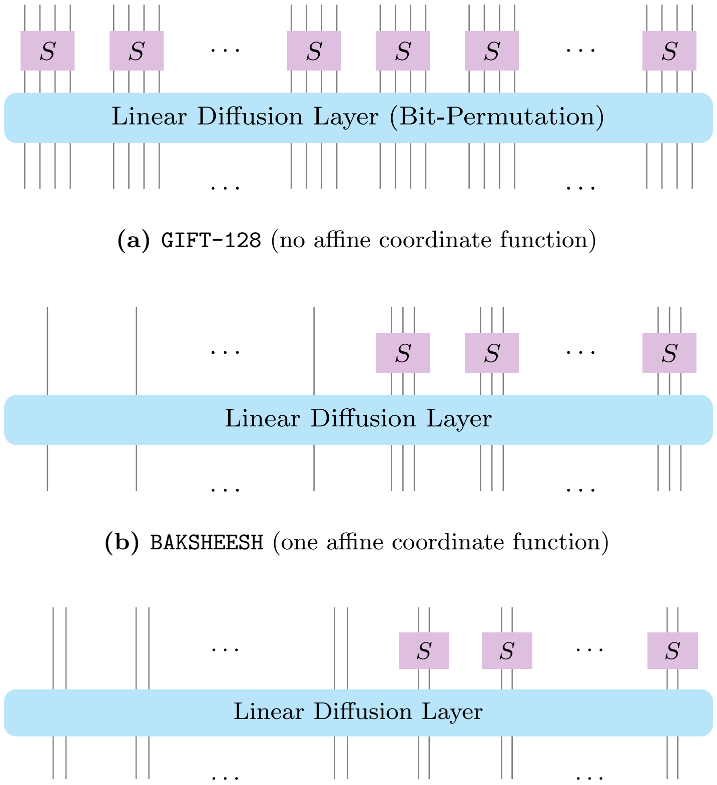
Another interesting feature, as can be noticed from [4, Table 6] that this cipher allows iterated linear trails. This goes against the traditional philosophy of limiting the number of (high



(a) Vanilla description (treating SBox as a whole)

(b) Equivalent description (using affine coordinate functions of SBox)

Figure 1: Structure of `DEFAULT-LAYER` one round for difference transition (schematic)



(a) `GIFT-128` (no affine coordinate function)

(b) `BAKSHEESH` (one affine coordinate function)

(c) `DEFAULT-LAYER` (two affine coordinate functions)

Figure 2: Equivalent schematic for one round (showing partial non-linear layer)

probability) iterated differential/linear trails. In reality, that design philosophy was conceived at an earlier time where the automated tools were not as pervasive. With the advancement of such tools, however, this is not an unavoidable philosophy any longer.

Also, since one coordinate function of the `BAKSHEESH` SBox is affine anyway, we recommend three-quarter key XOR for this cipher. To be more precise, the second most significant bit for each SBox input (which corresponds to the input difference `8`) can be skipped, while the rest 3 input bits of the SBoxes can be XORed with the respective round key.

3.4 Further Cryptographic Properties of LS SBox

In the rest, we assume the $n \times n$ SBox S unless noted otherwise. We use the shorthand notation $\Delta(x, \delta)$ to indicate the output difference corresponding to the input x and input difference δ, i.e., $S(x) \oplus S(x \oplus \delta) = \Delta(x, \delta)$.

Theorem 1 (Linear combination of LS). *If α and β are linear structures, then so is $\alpha \oplus \beta$ (with the constant output difference $\Delta(\cdot, \alpha \oplus \beta) = \Delta(\cdot, \alpha) \oplus \Delta(\cdot, \beta)$).*

Proof. We have $S(x) \oplus S(x \oplus \alpha) = \Delta(x, \alpha)$, (constant $\forall x$); and $S(x) \oplus S(x \oplus \beta) = \Delta(x, \beta)$, (constant $\forall x$). Now, $S(x) \oplus S(x \oplus \alpha \oplus \beta) = (S(x) \oplus S(x \oplus \alpha)) \oplus (S(x \oplus \alpha) \oplus S(x \oplus \alpha \oplus \beta)) =$

$\Delta(x, \alpha) \oplus \Delta(x \oplus \alpha, \beta)$, both of which are constant $\forall x$. This shows that $S(x) \oplus S(x \oplus \alpha \oplus \beta)$ is a constant $\forall x$. □

As Theorem 1 is true for any combination of linear structures, it shows that the number of LS is a power of 2.

Theorem 2. *There does not exist an SBox with 2^{n-1} many LS.*

The proof will be included later.

Note that Theorem 2 answers an open problem raised in the `DEFAULT` paper (the case for the 5-bit SBox was solved in [12]). Thus, the maximum number of LS an SBox can have is 2^{n-2}.

Theorem 3. *For an SBox with l linear structures, there are 2^l probability 1 transitions in its LAT, of which $l-1$ are linearly independent.*

The proof will be included later.

Theorem 4. *For SBox with l linear structures, the minimum non-zero value in its absolute LAT is 2^{l+1}.*

The proof will be included later.

Conjecture 1. If n is not a multiple of 3, then SBox S with maximum possible LBN $= \lceil \frac{2n}{3} \rceil$ has at least 1 non-trivial linear structure.

Conjecture 2. If an SBox has l LS, then at least 2^{l-1} rows in its DDT are pairwise identical.

In theory, similar results can be extended to LAT, ACT and BCT.

4 Conclusion

We take a deeper look at two recently proposed block ciphers, named `DEFAULT` and `BAKSHEESH`. Even though none of the ciphers claim to have a partially non-linear layer, these two ciphers do not actually posses a fully non-linear linear (as some of the bits passing through the substitution layer do not partake in a non-linear operation). This alternate angle allows us to revise the DFA security claim of `DEFAULT`.

In conclusion, we remark that the concept a partial non-linear layer seems to be a convergent evolution – a trait that has been evolved independently of one another more than once aiming at various justification. The main justification for this generally is some niche-specific cipher, though its evolution into the mainstream is spearheaded by `BAKSHEESH`).

Acknowlegement

This paper is a part of an ongoing discussion with Patrick Neumann, Christof Beierle and Gregor Leander from the Ruhr-Universität Bochum in Bochum, Germany.

References

1. Baksi, A.: Classical and Physical Security of Symmetric Key Cryptographic Algorithms. PhD thesis, School of Computer Science & Engineering, Nanyang Technological University, Singapore (2021) https://dr.ntu.edu.sg/handle/10356/152003. 3
2. Baksi, A. In: DEFAULT: Cipher-Level Resistance Against Differential Fault Attack. Springer Singapore, Singapore (2022) 177–216 1, 2
3. Baksi, A., Bhasin, S., Breier, J., Jap, D., Saha, D.: Fault attacks in symmetric key cryptosystems. Cryptology ePrint Archive, Report 2020/1267 (2020) 1
4. Baksi, A., Breier, J., Chattopadhyay, A., Gerlich, T., Guilley, S., Gupta, N., Isobe, T., Jati, A., Jedlicka, P., Kim, H., Liu, F., Martinásek, Z., Sakamoto, K., Seo, H., Shiba, R., Shrivastwa, R.R.: Baksheesh: Similar yet different from gift. Cryptology ePrint Archive, Paper 2023/750 (2023) https://eprint.iacr.org/2023/750. 1, 3
5. Baksi, A., Guilley, S., Shrivastwa, R.R., Takarabt, S.: From substitution box to threshold. Cryptology ePrint Archive, Paper 2023/633 (2023) https://eprint.iacr.org/2023/633. 3
6. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: Gift: A small present. Cryptology ePrint Archive, Report 2017/622 (2017) https://ia.cr/2017/622. 1
7. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The SKINNY family of block ciphers and its low-latency variant MANTIS. In: Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II. (2016) 123–153 1
8. Bilgin, B.: Threshold Implementations As Countermeasure Against Higher-Order Differential Power Analysis. PhD thesis, Katholieke Universiteit Leuven and University of Twente (2015) https://www.esat.kuleuven.be/cosic/publications/thesis-256.pdf. 3
9. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J., Seurin, Y., Vikkelsoe, C.: PRESENT: An ultra-lightweight block cipher. In: CHES. Volume 4727., Springer (2007) 450–466 1
10. Gérard, B., Grosso, V., Naya-Plasencia, M., Standaert, F.X.: Block ciphers that are easier to mask: How far can we go? (08 2013) 383–399 1
11. Nageler, M., Dobraunig, C., Eichlseder, M.: Information-combining differential fault attacks on DEFAULT. IACR Cryptol. ePrint Arch. (2021) 1374 3
12. Wadhwa, M., Baksi, A., Hu, K., Chattopadhyay, A., Isobe, T., Saha, D.: Finding desirable substitution box with SASQUATCH. Cryptology ePrint Archive, Paper 2023/742 (2023) https://eprint.iacr.org/2023/742. 6