Evolution of Linear Analysis on the “SAFER+” Block Cipher

Yeghiazar Grigoryan*, Gevorg Hunanyan† and Sergey Abrahamyan‡
*Institute for Informatics and Automation Problems of NAS RA, Yerevan, Armenia,
Email: e.grigoryan@iiap.sci.am
†Institute for Informatics and Automation Problems of NAS RA, Yerevan, Armenia,
Email: g.hunanyan@iiap.sci.am
‡Institute for Informatics and Automation Problems of NAS RA, Yerevan, Armenia,
Email: serj.abrahamyan@gmail.com

***Abstract*—SAFER+ is a modern block cipher that was submitted as a candidate for the Advanced Encryption Standard (AES). It has various applications and is considered to be one of the most secure block ciphers. All well-known attacks, including linear and differential cryptanalysis, have been applied to SAFER+ without revealing any vulnerabilities. In this paper, we review linear cryptanalysis attacks against SAFER+ and present additional data that may be of interest for the further development of linear cryptanalysis.**

***Keywords*—Linear Cryptanalysis, SAFER+, Block Cipher.**

I. Introduction

Linear cryptanalysis, which is one of the main cryptanalysis methods against block ciphers, was introduced by Gilbert, Chasee, and Tardy in 1991 [1], [2]. In 1994, Matsui applied it to DES and showed that it can mitigate exhaustive key search and break it using only 2^{45} known plaintext-ciphertext pairs. This result made linear cryptanalysis one of the most famous cryptanalysis methods against block ciphers.

Matsui adapted linear cryptanalysis to DES and similar block ciphers [3] as a theoretical method for analyzing block ciphers and determining key bits. The main idea is to find approximate linear relations between plaintext, ciphertext, and key bits to gain information about the partial keys. It is done by considering the equation:

$$\alpha \cdot X = \beta \cdot \mathcal{E}(X),$$

where X is the input and α and β denote the input and output masks for the encryption function, respectively. The $(\cdot)$ operation here is the dot product of the vector space $\mathbb{F}_2^n$. If the probability that this equation holds for randomly given x is different from $\frac{1}{2}$, then a sufficient number of plaintext-ciphertext pairs can be used to reveal one bit of information about the key bits involved in the equation. The approximation is then extended to the entire cipher. Matsui suggested two approaches, which he called Algorithm 1 and Algorithm 2. Algorithm 2 was then used to break 8-round and 16-round DES ciphers with 2^{21} and 2^{45} plaintext-ciphertext pairs, respectively.

Another approach for linear cryptanalysis is to generalize it with the sum of balanced functions. This principle is introduced by Harpes, Kramer, and Massey in [4], and the motivation behind it is to enhance Matsui’s principle for iterated ciphers. For this purpose Harpes *et al.* gives the idea of I/O sums for the i-th round of the cipher:

$$S^{(i)} = f_i(Y^{i-1}) \oplus g_i(Y^i),$$

where $f_i(Y^{i-1})$ is a balanced Boolean function with Y^{i-1} (output of $(i-1)$-th round) as input and $g_i(Y^i)$ a balanced Boolean function accordingly. These two functions are called the input and output functions of the I/O sum of the i-th round, respectively. For more rounds of the cipher, there is the idea of a multi-round I/O sum, which is nothing more than the sum of consecutive I/O sums:

$$S^{(1,\ldots,\rho)} = \bigoplus_{i=1}^{\rho} S^{(i)} = f_1(Y^{(0)}) \oplus g_\rho(Y^{(\rho)}).$$

If the key-mixing part in the encryption round is done by a group or quasigroup operation or mod-2 addition, then it is necessary to introduce the idea of homomorphic I/O sums, where the sum of the input and output functions is a homomorphism from the group with the key mixing operation to the cyclic group of order two. Here, similar to Matsui, the effectiveness of an I/O sum for the concerns of cryptanalysis is measured by estimating the probability bias of the function with an extra factor of 2, which is called the imbalance property of the sum, i.e. $0 \leq I(S^{(i)}) \leq 1$. Harpes *et al.* also gave the basic attack algorithm for known (plaintext, ciphertext) pairs attack based on the imbalance results of the I/O sum. In [4] Harpes enhanced their idea by adding a balanced function of the round key $(K^{(i)})$ to the sum, which the authors called a Threefold sum:

$$T^{(i)} = f_i(Y^{i-1}) \oplus g_i(Y^i) \oplus h_i(K^i).$$

II. Preliminaries

In this paper, we provide an overview of the application of linear cryptanalysis on SAFER+. In [9] Harpes presented a linear cryptanalysis of SAFER-K64, which has the same structure as SAFER+. Actually, [9] is a direct application of [4] on SAFER-K64. He showed that SAFER-K64 is secure

https://doi.org/10.51408/csit2025_37

against linear cryptanalysis after one and a half rounds. Below, we provide a short description of SAFER+.

A. Description of SAFER+

The SAFER+ block cipher was developed by Prof. J. Massey with Dr. M. Kyureghyan and Prof. G. Khachatryan in 1998 [5], and was nominated for Advanced Encryption Standard as a candidate. The block size of SAFER+ is 128 bits, which provided for plaintext and ciphertext, also user-selected keys could be in 128, 192, and 256 bit sizes. The encryption routine for SAFER+ consists of $8(12, 16)$ rounds for the user-choosen $128(192, 256)$ bit key length. The one round of encryption is illustrated in figure 1, and the following cases will describe the SAFER+ encryption round routine:

1) The round input (Y_{i_0}) is represented by a 16-byte array:
2) The first key addition by K_{2i-1} is done by mod-2 and mod-256:

$$Y_{i_1} := \{x_j \circ k^j_{2i-1}, \text{ where} \circ := \\ \oplus \ | j \in \{1,4,5,8,9,12,13\} \text{ and} \\ +_{256} \ | j \in \{2,3,6,7,10,11,14,15\}\}.$$

3) The non-linear layer process:

$$Y_{i_2} := \{NL(y_j), \text{ where} NL := \\ 45^{y_j} \ | j \in \{1,4,5,8,9,12,13\} \text{ and} \\ log_{45}(y_j) \ | j \in \{2,3,6,7,10,11,14,15\}\}.$$

Here, the NL functions are processed by modulo 257. In addition, the 256 value in the *exponent* function is represented by 0, and the value for 0 input in the *logarithm* function by 128.

4) The second key addition by K_{2i} key, where the indexes changed for mod-2 and mod-256 addition regarding the first key addition.
5) And the last part of the encryption round comes with linear transformation by an inverse matrix with entries from $\mathbb{Z}_{256}$ and 128×128 size, this is also done by 4 layers of 2-PHT and Armenian Shuffle permutations.

III. Review of Existing Results

K. Kyuregyan and M. Kyureghyan in [6] showed that similar to the original SAFER+, a modified version of SAFER+ is secure against the generalized linear cryptanalysis method introduced by Harpes *et al.* after only two rounds. The approach is to find effective homomorphic I/O sums for each of the half-rounds and combine them to yield an effective homomorphic I/O sum for the entire cipher.

A procedure for finding effective homomorphic I/O sums of multiple layers is described, and it is proved that this procedure does not yield effective homomorphic I/O sums for a cascade of half-rounds containing at least two PHT layers. K. Kyuregyan carried out the calculations for linear cryptanalysis of SAFER-256 in [7]. SAFER-256 has also been shown to be secure against linear cryptanalysis after three rounds.

The next effective approach was proposed by J. Nakahara, B. Preneel and J. Vandewalle [8]. They showed that the usage of non-homomorphic functions will yield stronger dependency of key bits and improved linear relations. The idea of using non-homomorphic functions in SAFER+ comes with splitting a round approximation into four parts of quarter rounds: the key mixing layers, the non-linear layer, and the linear matrix multiplication layer (PHT). With this enhancement of the principle of Harpes *et al.*, they were able to achieve a linear approximation of 2.75 rounds of SAFER+. In their calculations of the linear approximation, for the generation of linear relations for the PHT layer, they used linear hulls.

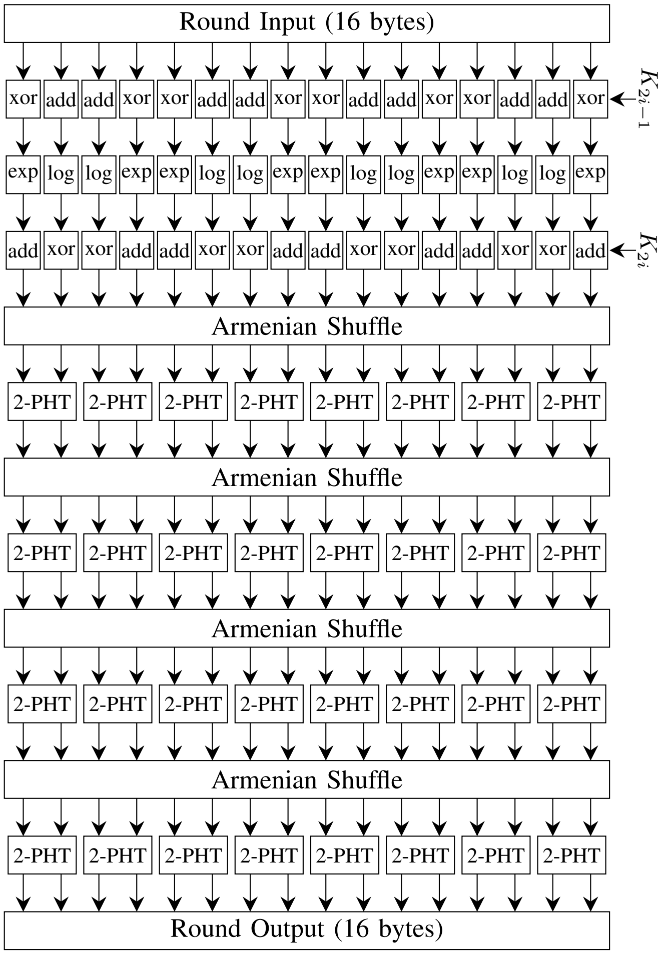
Round Input (16 bytes)
xor add add xor xor add add xor xor add add xor xor add add xor
K_{2i-1}
exp log log exp exp log log exp exp log log exp exp log log exp
add xor xor add add xor xor add add xor xor add add xor xor add
K_{2i}
Armenian Shuffle
2-PHT 2-PHT 2-PHT 2-PHT 2-PHT 2-PHT 2-PHT 2-PHT
Armenian Shuffle
2-PHT 2-PHT 2-PHT 2-PHT 2-PHT 2-PHT 2-PHT 2-PHT
Armenian Shuffle
2-PHT 2-PHT 2-PHT 2-PHT 2-PHT 2-PHT 2-PHT 2-PHT
Armenian Shuffle
2-PHT 2-PHT 2-PHT 2-PHT 2-PHT 2-PHT 2-PHT 2-PHT
Round Output (16 bytes)

Fig. 1. i-th round of SAFER+

The notion of a linear hull was introduced by K. Nyberg in [10], defined as the set of all linear trails that share the same input and output masks. In classical linear cryptanalysis (e.g., Matsui's method), one typically focuses on a single best trail and applies the piling-up lemma to combine round correlations, but Nyberg observed that many ciphers admit multiple distinct trails for a given input-output mask. The hull framework, therefore, aggregates all such trails: The net correlation of the approximation is computed by summing the contributions of each trail in the hull. This method often yields a larger effective bias than any individual trail alone.

Nakahara *et al.* explicitly applied Nyberg's linear hull technique to the PHT layer of SAFER+. For each fixed input-output mask on a two-byte PHT addition, they collected all single-path linear approximations that share that mask, treating this collection as a single linear hull (as defined by Nyberg). In practice, they restricted attention to the two least significant bits of each 2-byte PHT addition, since these bits yield the strongest biases. Summing the bias contributions of all trails in one hull often showed cancellation - some trails have positive deviation and others equal-magnitude negative deviation, which cancel out. This gives the aggregate (often small or zero) bias of the PHT-layer hull. They then combined each PHT-layer hull with the corresponding hulls from the nonlinear S-box and subkey layers to form full one-round linear approximations. In other words, instead of following a single trail per round, the authors summed over all trails (the hull) for that round before proceeding, thereby taking advantage of Nyberg's idea of aggregating biases.

In Table I, the current results of linear cryptanalysis for block ciphers of the SAFER family have been provided.

TABLE I
The SAFER+ Linear Cryptanalysis Results

Authors	Cryptanalysis Type	Rounds	Bias	Cipher
M. Kyureghyan, K. Kyureghyan [6]	Homomorphic I/O sum	2.5	$\approx 2^{-11}$	SAFER+ (modified version)
J. Nakahara, B. Preneel, J. Vandewalle [8]	Non-Homomorphic I/O sum	2.75	2^{-49}	SAFER+
C. Harpes [9]	Homomorphic I/O sum	1.5	$\approx 2^{-6}$	SAFER-K64

From Table I, it becomes clear that currently the best method has been provided by Nakahara *et al.* in [8].

IV. Calculation of LAT Table for SAFER+ Non Linear Functions

One of the primary properties in Linear Cryptanalysis is the Linear Approximation Table (LAT), whose entries are the biases for the S-box (non-linear function) of the cipher. The *exponential* and *logarithmic* functions' LAT should be calculated for analyzing the resistance of SAFER+ to the Linear Cryptanalysis. The bias refers to how much the output distribution of the S-box deviates from a uniform distribution:

$$\mathrm{P}[\alpha \cdot X \oplus \beta \cdot S(X) = 0] - \frac{1}{2}.$$

Each entry in LAT is calculated using input (α) and output (β) masks from $\mathbb{F}_2^n$ for an S-box and iterating over the domain elements of the function. We have computed LAT values for the *exponential/logarithmic* function. The highest absolute bias values are given in Table II.

Since the *logarithm* function is the inverse of the exponential, its LAT is the transpose of the LAT of the exponential function.

TABLE II
A Part of The Linear Approximation Table

α/β	23	32	52	80	AB	CC	D1	F1	FE
11	0	2	-2	2	10	2	16	-8	**44**
1B	2	2	2	2	10	-2	8	2	**-44**
26	0	-22	2	0	**42**	16	-14	-6	2
2D	2	8	2	0	**38**	-10	-2	0	-2
3A	0	**-46**	2	2	12	**38**	0	0	0
42	**-36**	2	-12	2	-2	8	6	-2	6
65	-8	2	2	2	4	-2	**36**	0	0
B3	0	4	0	2	-6	0	6	**-34**	-4
EF	-2	-4	0	**34**	-8	10	-6	-4	-6

V. Conclusion

Although linear cryptanalysis remains a powerful technique against block ciphers, SAFER has proven to be resilient to such attacks. The most effective known result, achieved by Nakahara *e*t al. in [5] successfully breaks only 2.75 out of 7 rounds.

References

[1] A. Tardy-Corfdir, H. Gilbert, "A Known Plaintext Attack of FEAL-4 and FEAL-6", *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, vol. 576, 1992.

[2] H. Gilbert, G. Chassé, "A Statistical Attack of the FEAL-8 Cryptosystem", *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, vol. 537, 1991.

[3] M. Matsui, "Linear Cryptanalysis Method for DES Cipher", *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, vol. 765, 1994.

[4] C. Harpes, G.G. Kramer, J.L. Massey, "A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-up Lemma", *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, vol. 921, 1995.

[5] J. L. Massey, G. H. Khachatrian, M. K. Kuregian, "Nomination of SAFER+ as candidate algorithm for the Advanced Encryption Standard (AES)", 1998.

[6] M. K. Kyureghyan, K. M. Kyuregyan, "Linear Cryptanalysis of Modified SAFER + Algorithm", *Mathematical Problems of Computer Science*, vol. 45, pp. 111–121, 2016.

[7] K. M. Kyuregyan, "Linear Cryptanalysis of SAFER-256", *Mathematical Problems of Computer Science*, vol. 45, pp. 127–137, 2016.

[8] J. Nakahara, B. Preneel, J. Vandewalle, "Linear Cryptanalysis of Reduced-Round Versions of the SAFER Block Cipher Family", *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, vol. 1978, 2001.

[9] C. Harpes, "A Generalization of Linear Cryptanalysis applied to SAFER", *Signal and Information Proc*, Swiss Federal Institute of Technology, Zürich, March 1995.

[10] K. Nyberg, "Linear approximation of block ciphers", *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, vol. 950, 1995