Linear Cryptanalysis of the SAFER Block Cipher Family*

Sergey Abrahamyan

Institute for Informatics and Automation Problems
Yerevan, Armenia
e-mail: serj.abrahamyan@gmail.com; seroj1983@yahoo.com

Melsik K. Kyureghyan

Institute for Informatics and Automation Problems
Yerevan, Armenia
e-mail:melsik@ipia.sci.am

ABSTRACT

This paper presents a linear cryptanalytic attack against the SAFER family of block ciphers. Linear cryptanalysis is a statistical well-known-plaintext attack that explores (approximate) linear relations between plaintext, ciphertext and subkey bits. These linear relations apply only to certain key classes. The results show that by considering non-homomorphic linear relations, more rounds of the SAFER block cipher family can be attacked. The new attacks pose no threat to any member of the SAFER family.

Keywords

Linear cryptanalysis, block chipper, approximate linear relation, plaintext, ciphertext, linear relation bias

1. INTRODUCTION

SAFER (Secure And Fast Encryption Routine) is a family of block ciphers, designed by Massey. The newest member of this family is the AES candidate SAFER+ [1] designed jointly with Khachatrian and Kuregian; SAFER+ has a 128-bit block size and variable key size versions of 128, 192 and 256 bits.

The more widespread, easy-to-deploy and better-understood an encryption algorithm is, the more attractive it becomes as a target for cryptanalysts. All SAFER family members, including SAFER+, SAFER++ [1, 2] have publicly available descriptions, are unpatented, royalty-free, with plenty of flexibility for different key sizes and block sizes, and are designed to be efficiently implementable in software. These are key features to make SAFER+ widely deployed. An example is the inclusion of SAFER+ for authentication purposes in Bluetooth [1]; this is the code-name for a technology specification for low-cost, short range radio links between mobile PC's, mobile phones and other portable devices.

An indispensable evidence of security of a cipher is its cryptaresistence against both types of cryptanalytic attacks differential and linear. Linear cryptanalysis is one of the two most widely used attacks on block ciphers introduced by Matsui in 1993 [3]. Linear cryptanalysis has proved to be a very effective general attack against ciphers, however it was weak against previous SAFER family of ciphers. We begin in the next section (Section 2) with a brief description of SAFER+. Section 3 introduces some terminology for our attack. Section 4 gives the details of our version of leaner cryptanalysis of SAFER+, which was carried out with the help of a software package that is used to find linear approximations. We close in section 5 with our conclusion.

*The research was supported by ISTC A-1451 project.

2. DESCRIPTION OF SAFER+

SAFER+ is a block cipher that operates on 128-bit plaintext blocks, considered as 16 bytes, under control of a user-selected key whose length may be chosen as 128 or 256 bits. SAFER+ consists of a round transformation iterated *r* times, followed by an output transformation. The number of rounds is *r* = 7, or 10 according as the key length is 128, or 256 bits, respectively. For this cipher, we will use the convention that bytes, i.e. 16-typles, are numbered from 1 to 16 and their bits, as usual, from 7 for the most significant bit to 0 for the least significant bit. Thus, if X is any eight-byte variable, we will write $X1, X2, X3, \ldots, X16$ for instance,

$$X1 = X1_7, X1_6, X1_5, X1_4, X1_3 X1_2, X1_1, X1_0.$$

The round function of an r-round iterated cipher SAFER+ is defined in Fig. 1.

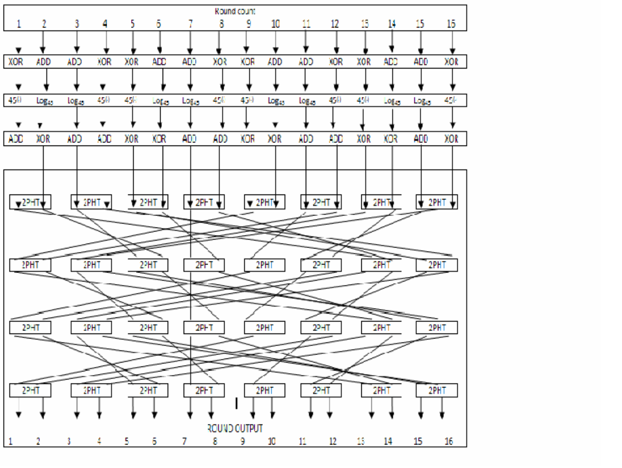

Figure 1: Schematic of the i-th round of cipher SAFER+

Let X denote the input and let Y denote the output of this round function. The round function consists of a cascade of

1. a byte-wise mixed XOR/Byte-Addition (XOR/ADD) of 8 input bytes and 8 key bytes, viz., the first part K_L of the round key, – its output is $U = XOR/ADD(X, K_L)$;
2. a non-liner layer, where each byte is subjected to either the non linear function $EXP: X \to 45^X$ modulo 257 (with the convention that when X =128 then 45^{128} mod257=256 is represented by 0) or its inverse function LOG – its output is $V = NL(U)$;
3. a byte-wise mixed Byte-Addition/ XOR

(ADD/XOR) of 8 input bytes and 8 key bytes, viz., the second part K_R of the round key – its output is $W = ADD/XOR(V, K_R)$, and

4. a Pseudo-Hadamard Transformation PHT, consisting of a four level "liner layer" of boxes labeled "2-PHT" such that $Y = PHT(W)$, i.e.

$Y_1=2W_1+W_2+W_3+W_4+4W_5+2W_6+W_7+W_8+2W_9+2W_{10}+4W_{11}+2W_{12}+4W_{13}+4W_{14}+16W_{15}+8W_{16}$

$Y_2=2W_1+W_2+W_3+W_4+4W_5+2W_6+W_7+W_8+W_9+W_{10}+2W_{11}+W_{12}+2W_{13}+2W_{14}+8W_{15}+4W_{16}$

$Y_3=W_1+W_2+4W_3+2W_4+2W_5+2W_6+4W_7+2W_8+16W_9+8W_{10}+4W_{11}+4W_{12}+2W_{13}+W_{14}+W_{15}+W_{16}$

$Y_4=W_1+W_2+4W_3+2W_4+W_5+W_6+2W_7+W_8+8W_9+4W_{10}+2W_{11}+2W_{12}+2W_{13}+W_{14}+W_{15}+W_{16}$

$Y_5=16W_1+8W_2+2W_3+2W_4+4W_5+2W_6+4W_7+4W_8+W_9+W_{10}+4W_{11}+2W_{12}+W_{13}+W_{14}+2W_{15}+W_{16}$

$Y_6= W_1+4W_2+W_3+W_4+2W_5+W_6+2W_7+2W_8+W_9+W_{10}+4W_{11}+2W_{12}+W_{13}+W_{14}+2W_{15}+W_{16}$

$Y_7= W_1+2W_2+4W_3+2W_4+4W_5+4W_6+16W_7+8W_8+2W_9+W_{10}+W_{11}+W_{12}+4W_{13}+2W_{14}+W_{15}+W_{16}$

$Y_8= {}_1+W_2+2W_3+W_4+2W_5+2W_6+8W_7+4W_8+2W_9+W_{10}+W_{11}+W_{12}+4W_{13}+2W_{14}+W_{15}+W_{16}$

$Y_9= 4W_1+2W_2+4W_3+4W_4+16W_5+8W_6+2W_7+2W_8+W_9+W_{10}+2W_{11}+W_{12}+W_{13}+W_{14}+4W_{15}+2W_{16}$

$Y_{10}= 2W_1+W_2+2W_3+2W_4+8W_5+4W_6+W_7+W_8+W_9+W_{10}+2W_{11}+W_{12}+W_{13}+W_{14}+4W_{15}+2W_{16}$

$Y_{11} =4W_1+4W_2+16W_3+8W_4+W_5+W_6+2W_7+W_8+4W_9+2W_{10}+W_{11}+W_{12}+4W_{13}+2W_{14}+2W_{15}+2W_{16}$

$Y_{12}=2 W_1+2W_2+8W_3+4W_4+W_5+W_6+2W_7+W_8+4W_9+2W_{10}+W_{11}+W_{12}+2W_{13}+W_{14}+W_{15}+W_{16}$

$Y_{13}= W_1+W_2+2W_3+W_4+W_5+W_6+4W_7+2W_8+4W_9+4W_{10}+16W_{11}+8W_{12}+2W_{13}+2W_{14}+4W_{15}+2W_{16}$

$Y_{14}= W_1+W_2+2W_3+W_4+W_5+W_6+4W_7+2W_8+2W_9+2W_{10}+8W_{11}+4W_{12}+W_{13}+W_{14}+2W_{15}+W_{16}$

$Y_{15}= 4W_1+2W_2+W_3+W_4+2W_5+W_6+W_7+W_8+4W_9+2W_{10}+2W_{11}+2W_{12}+16W_{13}+8W_{14}+4W_{15}+4W_{16}$

$Y_{16}= 4W_1+2W_2+W_3+W_4+2W_5+W_6+W_7+W_8+2W_9+W_{10}+W_{11}+W_{12}+8W_{13}+4W_{14}+2W_{15}+2W_{16}$

Table 1

3. PRELIMINARIES

This section we follow the terminology and notation for linear attacks on SAFER+ ciphers.

Let $X = (X1, X2, X3, \ldots X16)$ denote an 16-byte input and $Y = (Y1, Y2, Y3, \ldots Y16)$ an 16-byte output to a round of block cipher, and let $K^i = (K^i{}_1, K^i{}_2, \ldots, K^i{}_{16},)$ and $K^{i+1} = (K^{i+1}{}_1, K^{i+1}{}_2, \ldots, K^{i+1}{}_{16},)$ denote the first and the second keys, respectively, of the i-th round of a block cipher.

Let $\boxplus$ denote some addition operation between the last two bits of plaintext and key bytes with the same position number, i.e. $Xij \boxplus Kij = Xij_1 \oplus Kij_1$ when $ij = 1,4,5,8,9,12,13,1,6$ and $Xij \boxplus Kij = Xij_1 \oplus Xij_1 \oplus Kij_1$ when $ij = 2,3,6,7,10,11,14,15$.

Now define the function $F(Xi1, Xi2, \ldots, Xij, Ki1, ki2, \ldots, kij)$ as follows:

Definition 1 The function $F(Xi1, Xi2, \ldots, Xij, Ki1, ki2, \ldots, kij) = (Xi1 \boxplus Ki1) \oplus (Xi2 \boxplus Ki2) \oplus (Xi3 \boxplus Ki3) \oplus \cdots + \oplus (Xij \boxplus Kij)$.

Define the function $G(ik)$ linking the ik-th byte of a *plaintext* and the bits of a *ciphertext* as follows:

Definition 2. $G(ik) = Yi1_1 \oplus Yi2_1 \oplus \cdots \oplus YiL_1$, where ik denote the ik-th input byte and $Yi1_1, Yi2_1, \cdots, YiL_1$ denote those bites of a ciphetext that have been affected by penultimate bits of Xik byte (see Table 1). For example

$$Y2 = 2X1 + X2 + X3 + X4 + 4X5 + 2X6 + X7 + X8 + X9 + X10 + 2X11 + X12 + 2X13 + X14 + 8X15 + 4X16$$

If the coefficient of Xik is ≤ 2 then Y_i has been effected by Xik_1.

Definition 3 We call a relation of the type

$$F(Xi1, Xi2, \ldots, Xij, Ki1, ki2, \ldots, kij) = G(i1) \oplus G(i2) \oplus \cdots \oplus G(ij) \quad (1)$$

a *linear relation or an approximate (linear) relation (*as it is accepted conventionally in cryptography).

Let N denote the set $|N| = n$ of all known plaintexts and let M denote the set of *plaintexts* for which a linear relation holds and write $|M| = m$.

Consider the following probability:

$$P = \mathbf{Pr}(F(Xi1, Xi2, \ldots, Xij, Ki1, ki2, \ldots, kij) \; G(i1) \oplus G(i2) \oplus \cdots \oplus G(ij))/n = m/n$$

where n denotes the number of known plaintexts; $Ki1, Ki2, \ldots, Kij$ are the fixed key bytes. P indicates the probability with which *plaintexts* and corresponding *ciphertexts* meet a linear relation.

The absolute value of $e = |P - 1/2|$ is called *bias of linear relation.*

4. OUR VERSION OF LINEAR CRYPTANALISIS OF SAFER+

A binary sequence of length n is said to be the *key* of an n-byte block cipher, if it doesn't include a subsequence of more than 7 successive 0's or 1's.

Let $k \subset \{B^n / B^n = B \times B \times B \cdots \times B, \quad B \in \{0,1\}\}$ be the set of all possible keys of a block cipher. Our experimental results have shown that block ciphers produce nearly identical behavior for almost all the values of the keys, i.e. they are mainly 'homomorphic', by which we mean that for a fixed key the bias coefficient e between *plaintext, ciphertext* and *key* bits lies in the range $0.00001 < e < 0.0001$ (depending on the number of plaintexts this bias coefficient may be even smaller) and in the range $0 \le e < 0.00001$ for a very small number of keys.

The observed property suggests that it is could be reasonable to split the the set of all possible keys into two subsets. We built our scheme of linear cryptanalysis against block ciphers mainly based on this feature. A detailed description of the attack is given below.

With the help of a software package ('Bias Tracker' that runs under Armenian Grid infrastructure), provided to conduct linear cryptanalysis of block ciphers by exploring approximate (linear) relations (i.e. relations with nonzero bias), a cryptanalyst may chose the list of keys with the bias $0 \le e < 0.00001$ and the set of *plaintexts* that produce this bias (actually availability of the first plaintext is required, since the following plaintexts are sequentially generated from the first one). Then the cryptanalyst consequently choses a keys from the key list and the corresponding plaintext, and generates the sequential plaintexts by using the above-described technique. The generated *plaintext*s are input to block cipher and the corresponding *ciphertext*s are produced. For all known plaintexts, ciphertexts and the fixed key k we count the bias. If the computed bias is identical to key bias then it is most likely to be the sought key. Then we input this key and some amount of known plaintexts to block cipher. If the resulting ciphertexts are identical to the checked (true) ciphertexts, then the key is broken; otherwise we consider the next key.

5. Preliminary Conclusions based on Experimental Results

For effective realization of a linear cryptanalytic attack it is important to have a right choice of minimal number of known plaintexts. Clearly, only psedorandom plaintexts are required. For our scheme the plaintext are chosen as follows. We take an 16-byte array, each byte including numbers in the range 0-255 as the known plaintext. Every sequential plaintext is generated from the former one as follows:

$$X_i^j = f(x) = \begin{cases} 45^{X_j^{i-1}} \ \mathbf{mod}\, 257 & X_j^{i-1} \in Z_{256} \setminus \{0\} \\ 128 & X_j^{i-1} \end{cases}$$

$$j = 1,4,5,8,9,12,13,16$$

and

$$X_i^j = f(x) = \begin{cases} \mathbf{log}_{45^{X_j^{i-1}}} \ \mathbf{mod}\, 257 & X_j^{i-1} \in Z_{256} \setminus \{0\} \\ 128 & X_j^{i-1} \end{cases}$$

$$j = 2,3,6,7,10,11,14,15$$

where X_i^j is the j -th byte of the i -th *plaintext.*

Next the content of 1-4 , 5-8, 9-12, 13-16 bytes is combined and cyclically shifted by 4 bits. Experimental data indicate that plaintexts generated in such manner are pseudorandom.

Let we are given a key k and some amount of plaintexts. For the given key k and the given plaintexts we need to determine the probability with which the linear relation holds and the bias e. Observe that the bias changes substantially with the increase of the amount of plaintexts. This conclusion is drawn on the background of a great many tests, performed on 1.000. 000, 10.000.000and 100. 000. 000 plaintexts. Our experiments show that for the case of 10.000.000 known plaintexts the keys having the bias $0 \le e < 0.00001$ occur not frequently. This enables a cryptanalyst to handle a larger number of sets of keys with such bias and, as a result may offer a significant improvement in the efficiency of an attack on the SAFER family of block ciphers.

REFERENCES

[1] J. L. Massey, G. H. Khachatrian, M. K. Kuregian, ``Nomination of SAFER+ as Candidate Algorithm for the Advanced Encryption Standard (AES)", NIST AES Proposal, 1998.

[2] J. L. Massey, G. H. Khachatrian and M. K. Kuregian, Nomination of SAFER++ as Candidate Algorithm for the New European Schemes for Signatures, Integrity, and Encryption (NESSIE), Submission document from Cylink Corporation, 2000.

[3] M. Matsui, "Linear cryptanalysis method for DES cipher," Advances in Cryptology, Proceedings Eucocrypt'93, LNCS 765, T. Helleseth, Ed., Springer-Verlag, pp. 386-397, 1994.