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 cipher, 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.

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-tuples, 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 \( X = (X_1, X_2, X_3, \ldots, X_{16}) \) for instance;

\[
X_1 = X_{16}, X_{15}, X_{14}, X_{13}, X_{12}, X_{11}, X_{10}, X_9.
\]

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

2.1. Round Function
The round function of \( r \)-round iterated block cipher SAFER+ 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-linear layer, where each byte is subjected to the non linear function \( EXP : X \rightarrow 45^X \mod 257 \) (with the convention that when \( X = 128 \) then \( 45^{128} \mod 257 = 256 \) is represented by 0) or its inverse function \( LOG \) – its output is \( V = NL(U) \);
3. a byte-wise mixed Byte-Addition/ XOR

\[ V = NL(U) \]

The research was supported by ISTC A-1451 project.
3. PRELIMINARIES

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

Let \( X = (X_1, X_2, X_3, \ldots, X_{16}) \) denote an 16-byte input and \( Y = (Y_1, Y_2, Y_3, \ldots, Y_{16}) \) an 16-byte output to a round of block cipher, and let \( K = (K_1, K_2, \ldots, K_{16}) \) 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 \( \oplus \) denote some addition operation between the last two bits of plaintext and key bytes with the same position number, i.e.

\[
X_{ij} \oplus K_{ij} = X_{ij} \oplus K_{ij}
\]

when \( ij = 1, 4, 5, 8, 9, 12, 13, 16 \) and

\[
X_{ij} \oplus K_{ij} = X_{ij} \oplus K_{ij} \oplus K_{ij}
\]

when \( ij = 2, 3, 6, 7, 10, 11, 14, 15 \).

Now define the function

\[
F(X_{i1}, X_{i2}, \ldots, X_{ij}, K_{i1}, k_{i2}, \ldots, k_{ij}) = (X_{i1} \oplus K_{i1}) \oplus (X_{i2} \oplus K_{i2}) \oplus (X_{i3} \oplus K_{i3}) \oplus \cdots \oplus (X_{ij} \oplus K_{ij})
\]

Definition 1 The function \( F(X_{i1}, X_{i2}, \ldots, X_{ij}, K_{i1}, k_{i2}, \ldots, k_{ij}) \) as follows:

\[
(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 box” of layers labeled “2-PHT” such that \( Y = PHT(W) \), i.e.

\[
Y_1 = 2W_1 + W_2 + W_3 + W_4 + 2W_5 + W_6 + 2W_7 + 2W_8 + 2W_9 + 2W_{10} + 2W_{11} + 2W_{12} + 2W_{13} + 2W_{14} + 2W_{15} + 2W_{16}
\]

\[
Y_2 = 2W_1 + 2W_2 + W_3 + 2W_4 + W_5 + 2W_6 + 2W_7 + 2W_8 + 2W_9 + 2W_{10} + 2W_{11} + 2W_{12} + 2W_{13} + 2W_{14} + 2W_{15} + 2W_{16}
\]

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

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

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

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

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

\[
Y_8 = 2W_1 + 4W_2 + 4W_3 + 4W_4 + 4W_5 + 4W_6 + 4W_7 + 4W_8 + 4W_9 + 4W_{10} + 4W_{11} + 4W_{12} + 4W_{13} + 4W_{14} + 4W_{15} + 4W_{16}
\]

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

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

\[
Y_{11} = 4W_1 + 4W_2 + 4W_3 + 4W_4 + 4W_5 + 4W_6 + 4W_7 + 4W_8 + 4W_9 + 4W_{10} + 4W_{11} + 4W_{12} + 4W_{13} + 4W_{14} + 4W_{15} + 4W_{16}
\]

\[
Y_{12} = 2W_1 + 2W_2 + 2W_3 + 2W_4 + 2W_5 + 2W_6 + 2W_7 + 2W_8 + 2W_9 + 2W_{10} + 2W_{11} + 2W_{12} + 2W_{13} + 2W_{14} + 2W_{15} + 2W_{16}
\]

\[
Y_{13} = W_1 + 2W_2 + 2W_3 + 2W_4 + 2W_5 + 2W_6 + 2W_7 + 2W_8 + 2W_9 + 2W_{10} + 2W_{11} + 2W_{12} + 2W_{13} + 2W_{14} + 2W_{15} + 2W_{16}
\]

\[
Y_{14} = W_1 + 2W_2 + 2W_3 + 2W_4 + 2W_5 + 2W_6 + 2W_7 + 2W_8 + 2W_9 + 2W_{10} + 2W_{11} + 2W_{12} + 2W_{13} + 2W_{14} + 2W_{15} + 2W_{16}
\]

\[
Y_{15} = 4W_1 + 4W_2 + 4W_3 + 4W_4 + 4W_5 + 4W_6 + 4W_7 + 4W_8 + 4W_9 + 4W_{10} + 4W_{11} + 4W_{12} + 4W_{13} + 4W_{14} + 4W_{15} + 4W_{16}
\]

\[
Y_{16} = 4W_1 + 4W_2 + 4W_3 + 4W_4 + 4W_5 + 4W_6 + 4W_7 + 4W_8 + 4W_9 + 4W_{10} + 4W_{11} + 4W_{12} + 4W_{13} + 4W_{14} + 4W_{15} + 4W_{16}
\]

Table 1

4. OUR VERSION OF LINEAR CRYPTANALYSIS 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 \( k \subseteq \{B^2/B^n = B \times B \times B \times \cdots \times B \mid B \in \{0,1\}\} \) 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 \( 0 > e > 0.00001 \) 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 $0 \leq e < 0,00001$ 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 plaintexts are input to block cipher and the corresponding ciphertexts 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 pseudorandom 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:

$$X_j' = f(x) = \begin{cases} \frac{45}{X_j^{-1}} \mod 257 & X_j^{-1} \in Z_{256} \setminus \{0\} \\ 128 & X_j^{-1} \end{cases}$$

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

and

$$X_j' = f(x) = \begin{cases} \frac{\log}{X_j^{-1}} \mod 257 & X_j^{-1} \in Z_{256} \setminus \{0\} \\ 128 & X_j^{-1} \end{cases}$$

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

where $X_j'$ 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, 10,000,000 and 100, 000, 000 plaintexts. Our experiments show that for the case of 10,000,000 known plaintexts the keys having the bias $0 \leq e < 0,00001$ 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