Differential-Linear and Impossible Differential Cryptanalysis of Round-reduced Scream

Keywords: Linear cryptanalysis, differential cryptanalysis, differential-linear cryptanalysis, impossible differential cryptanalysis

Abstract: In this work we focus on the tweakable block cipher Scream, We have analysed Scream with the techniques, which previously have not been applied to this algorithm, that is differential-linear and impossible differential cryptanalysis. This is work in progress towards a comprehensive evaluation of Scream. We think it is essential to analyse these new, promising algorithms with a possibly wide range of cryptanalytic tools and techniques. Our work helps to realize this goal.

1 INTRODUCTION

A block cipher is one of the most important primitive of modern cryptography. A conventional block cipher has two inputs — a *plaintext (or message)* $M \in \{0,1\}^n$, a *key* $K \in \{0,1\}^k$ and produces a single output — a *ciphertext* $C \in \{0,1\}^n$ (seeFigure 1(a)). Therefore we can describe a block cipher as

$$E : \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n \qquad (1)$$

Compared to conventional block cipher, a tweakable block cipher takes an additional input called *tweak* along with the usual inputs — message and key (see Figure 1(b)) and maps the inputs to the ciphertext:

$$\tilde{E} : \{0,1\}^n \times \{0,1\}^t \times \{0,1\}^k \rightarrow \{0,1\}^n \qquad (2)$$

The tweak plays a very similar role as a nonce in the OCB mode or an initialization vector in the CBC mode.

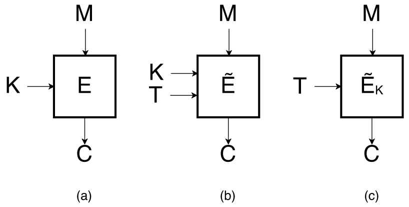

Figure 1: (a) Standard block cipher encrypts a message M under control of a key K to produce a ciphertext C. (b) Tweakable block cipher encrypts a message M under control of a key K and a "tweak" T to produce a ciphertext C. (c) Here the key K is shown inside the box.

The main purpose behind introducing a tweak is to bring functionality of a nonce (or initialization vector) down to the primitive block-cipher level, instead of incorporating it only at the higher modes-of-operation levels (Liskov et al., 2011). An extra cost of making a block cipher "tweakable" is small, so it is easier to design and prove modes of operation based on tweakable block ciphers. In this work we focus on the tweakable block cipher Scream (Grosso et al.,). An interesting and distinctive feature of Scream is that the algorithm has been designed to be secure against side-channel attacks. A side-channel attack is a way of exploiting information obtained from a physical implementation of the cryptosystem. Such information could be power or time consumption, area of memory access, electromagnetic radiation or even sound made by a device. Two techniques taken into consideration by Scream designers are differential power analysis (Kocher et al., 1999) and electro-magnetic analysis (Gandolfi et al., 2001).

Related work

Leander et al. presented a paper (Leander et al., 2015), where they introduced a generic algorithm to detect invariant subspaces and with this technique they cryptanalysed iSCREAM — an authenticated cipher based on a variant of Scream. Their attack is on a full cipher yet in a weak- or related-key model. A year later, at Asiacrypt 2016, an attack called the non-linear invariant attack was introduced (Todo et al., 2016). In that paper authors showed how to distinguish the full version of tweakable block cipher i-Scream, Scream and Midori64 in a weak key setting. For the authenticated encryption schemes SCREAM and i-SCREAM, the plaintext can be practically recovered only from the ciphertext in the nonce-respecting setting.

Our Contribution

To have a reliable evaluation of a new promising ciphers, such as Scream, third-party cryptanalysis is essential. Our goal is to analyse Scream with the techniques, which have not been considered or fully explored against Scream. In this work we focus on differential-linear and impossible-differential cryptanalysis and apply them to round-reduced variants of the cipher. First we propose a linear approximation for 5 rounds with the bias $\varepsilon = 2^{-49}$, upon which we build the 5-round key recovery attack. A linear approximation can be extended with a differential part, which is known as differential-linear analysis and it lets us mount the theoretical attack for 5 rounds with the complexity 2^{116}. Finally, we show an impossible differential path for 4 rounds obtained through the miss-in-the-middle approach.

2 SCREAM DESCRIPTION

The tweakable block cipher Scream is based on the LS-design variant (Grosso et al., 2014) known as TLS-design. The state is represented as an $s \times l$ matrix, where each element of the matrix represents a bit. Therefore a size of the block is $n = s \times l$ and Scream has a block size of $8 \times 16 = 128$ bits. The state x is updated by iterating N_s steps, where each step has N_r rounds as shown in Algorithm 1. A number of steps can vary and it serves as the security margin parameter. In the pseudo-code given below a plaintext is denoted by P, whereas TK (tweakey) is a simple linear combination of a tweak T and the master key K. In Scream, both key and tweak are 128 bits long.

Algorithm 1 TLS-design with $l-$bit L-boxes and $s-$bit S-boxes ($n = l \times s$).

```
$x = x \oplus TK(0)$          ▷ Set plaintext to all-zero vector
for $0 < \sigma \leq N_s$ do
    for $0 < \rho \leq N_r$ do
      $r = 2.(\sigma - 1) + \rho$
        for $0 \leq j < l$ do                    ▷ S-box Layer
            $x[*, j] = S[x[*, j]]$;
        end for
      $x = x \oplus C_r$;                      ▷ Constant addition
        for $0 \leq i < s$ do                    ▷ L-box Layer
            $x[i, *] = L[x[i, *]]$;
        end for
    end for
      $x = x \oplus TK(\sigma)$                ▷ Tweakey addition
end for
return x
```

The round constant $C(r)$ is defined as

$$C(r) = 2199 \times r(\bmod 216) \tag{3}$$

To calculate tweakeys (TK), first the tweak is divided into 64-bit halves, i.e., $T = t_0 || t_1$ and then tweakeys are calculated as follows:

$$TK(\sigma = 3i) = K \oplus (t_0 \parallel t_1), \tag{4}$$

$$TK(\sigma = 3i+1) = K \oplus (t_0 \oplus t_1 \parallel t_1), \tag{5}$$

$$TK(\sigma = 3i+2) = K \oplus (t_1 \parallel t_0 \oplus t_1). \tag{6}$$

3 LINEAR APPROXIMATION FOR 5-ROUND SCREAM

Linear cryptanalysis was introduced by Matsui (Matsui, 1993) and since then it has become a powerful cryptanalytic technique. The main idea behind linear cryptanalysis is to construct a linear approximation which describes a relation between input (plaintext) and output (ciphertext) bits. For a secure cipher we expect that such a relation holds with probability 0.5 (bias $\varepsilon = 0$) and we try to find an approximation where $\varepsilon \neq 0$. That would mean that the algorithm exhibits a non-random behaviour and potentially it could be converted to some attacks, such as the key recovery attack.

To construct a linear approximation for (round-reduced) Scream we proceed as follows. First, we examine the linear approximation table for the Scream S-box and choose the approximation with the highest bias. We find that the approximation $in_8 = out_8$ (8th input bit of the S-box equals 8th output bit) has the highest bias, namely 2^{-3}. There are 16 columns in the Scream state, hence 16 S-boxes in the S-box layer. We examine 2^{16} initial states for our linear approximation, where each S-box is either inactive or its 8th bit is active. In the subsequent rounds we always use the same S-box approximation ($in_8 = out_8$). A total bias is calculated using a formula introduced by Matsui (Matsui, 1993).

$$\varepsilon_{1,2,3\ldots15} = 2^{n-1} \prod_{i=0}^{i=15} \varepsilon_i \tag{7}$$

For 5 rounds, the best approximation we found has the bias $\varepsilon = 2^{-49}$ with 24 active S-boxes. Table 1 shows this linear approximation. We also investigate more rounds, for example 6-round approximation obtained by the same method has a total bias 2^{-65}. However, as a number of plaintext required for the key recovery attack is typically proportional to ε^{-2}, for 6 rounds (or more) we exceed the exhaustive search bound 2^{128} and analysis becomes much less meaningful.

Table 1: Linear approximation for the 5-round Scream. (Each column of the state is encoded as two hexadecimal numbers.)

00 80 00 00 80 00 00 00 00 80 00 00 00 00 80 00
↓
S-box Layer (active S-boxes: 4, bias: 2^{-9})
↓
00 80 00 00 80 00 00 00 00 80 00 00 00 00 80 00
↓
L-box Layer
↓
00 00 00 00 80 80 80 00 00 00 80 00 00 00 00 00
↓
S-box Layer (active S-boxes: 4, bias: 2^{-9})
↓
00 00 00 00 80 80 80 00 00 00 80 00 00 00 00 00
↓
L-box Layer
↓
00 80 00 80 80 00 00 80 80 00 00 80 00 80 00 80
↓
S-box Layer (active S-boxes: 8, bias: 2^{-17})
↓
00 80 00 80 80 00 00 80 80 00 00 80 00 80 00 80
↓
L-box Layer
↓
80 00 00 00 00 00 80 00 00 00 80 00 00 80 00 00
↓
S-box Layer (active S-boxes: 4, bias: 2^{-9})
↓
80 00 00 00 00 00 80 00 00 00 80 00 00 80 00 00
↓
L-box Layer
↓
00 00 80 00 00 80 00 00 00 80 80 00 00 00 00 00
↓
S-box Layer (active S-boxes: 4, bias: 2^{-9})
↓
00 00 80 00 00 80 00 00 00 80 80 00 00 00 00 00
↓
L-box Layer
↓
80 80 80 80 00 00 80 80 80 00 00 00 80 00 00 00

3.1 5-round key recovery attack

We can use a linear approximation we constructed to recover the secret key. First, we partially encrypt the first S-box layer by guessing some key bits, specifically the plaintext bits are XORed with the guessed subkeys and the result is run forward through the S-box. We need to guess these bits, which are needed to calculate values of bits involved in the linear approximation. Table 2 shows the details. For each subkey guess we create a counter and it is incremented once the linear approximation holds. A counter with a value which differs the most from a half of a number of plaintext/ciphertext pairs corresponds to the correct subkey guess.

Table 2: Initial and final states of the 4.5-round linear approximation.

00 80 00 00 80 00 00 00 00 80 00 00 00 00 80 00
↓
4.5-Rounds
↓
80 80 80 80 00 00 80 80 80 00 00 00 80 00 00 00

The above approximation has a total bias $\varepsilon = 2^{-41}$ and a number of plaintext/ciphertext pairs needed to detect the bias is $\varepsilon^{-2} = 2^{82}$. Active input bits in the linear approximation are placed in four different columns of the state (see Table 2). Therefore, we need to guess $4 * 8 = 32$ key bits, which gives 2^{32} possible combinations. For each combination we check 2^{82} plaintext/ciphertext pairs, so the time complexity of our key-recovery attack is $2^{82+32} = 2^{114}$.

By this procedure and with the presented 4.5-round linear approximation we extract 32 key bits. To recover more bits, we just repeat the procedure but with a different approximation, where input active bits are placed in different columns.

Comparison with an automated tool In (Dobraunig et al., 2015) a heuristic tool for finding linear characteristics was presented. The tool is inspired by SAT solvers and it was applied to modern authenticated ciphers. We used this tool to find good linear approximations for Scream and compare the results with our approach. For 5 rounds, the tool provides the approximation with bias $2^{-50.71}$ with 22 active S-boxes, while our approach leads to the characteristic with bias 2^{-49} and 24 S-boxes. Generally, we find the results similar and we argue that our relatively simple procedure for building linear approximations is comparable with this much sophisticated tool.

4 DIFFERENTIAL-LINEAR CRYPTANALYSIS OF ROUND-REDUCED SCREAM

Differential cryptanalysis was introduced (publicly) by Biham and Shamir (Biham and Shamir, 1990) in

Table 3: 1.5-round differential path with probability 1

00 00 00 00 00 00 00 00 80 00 00 00 00 00 00 00
↓
S-box Layer
↓
00 00 00 00 00 00 00 00 80 00 00 00 00 00 00 00
↓
L-box Layer
↓
?? ?? 00 ?? 00 00 ?? 00 00 ?? ?? 00 00 00 ?? 00
↓
S-box Layer
↓
?? ?? 00 ?? 00 00 ?? 00 00 ?? ?? 00 00 00 ?? 00

Table 4: Linear approximation covering 2.5 rounds

00 00 80 80 00 00 00 00 00 80 00 80 80 00 80 00
↓
L-box Layer
↓
00 00 00 00 00 80 00 80 00 00 80 00 80 80 80 00
↓
S-box Layer (active S-boxes: 6, bias: 2^{-13})
↓
00 00 00 00 00 80 00 80 00 00 80 00 80 80 80 00
↓
L-box Layer
↓
00 00 00 00 80 00 00 00 00 00 00 80 00 00 00 00
↓
S-box Layer (active S-boxes: 2, bias: 2^{-5})
↓
00 00 00 00 80 00 00 00 00 00 00 80 00 00 00 00
↓
L-box Layer
↓
80 00 00 80 80 00 00 00 00 00 00 80 00 80 00 80

1990 and is still one of the most powerful attacks on a wide range of cryptographic algorithms. In 1994 Langford and Hellman(Langford and Hellman, 1994) described a combination of linear and differential analysis known as differential-linear cryptanalysis.

In this section we apply differential-linear cryptanalysis to the round-reduced Scream cipher. We follow a typical scheme in this kind of attacks, namely first we create a differential path with probability 1 and then extend it by a linear part. Our differential path covers 1.5 rounds, please see Table 3. After the second S-box layer, there are still some bits with known differences. Using these known bits, we build the linear approximation as shown in Table 4.

5-round key recovery attack

This attack uses a differential path with probability 1 to set up a linear relation between two parallel instantiations of the cipher. A linear approximation involves the bits after 1.5 rounds so we have not a direct access to their values. However, we know the XOR difference between these bits and consequently the difference between ciphertext bits involved in the linear approximation. Therefore, to filter out the key guesses we check the linear relation between ciphertext bits.

In the attack we peel off the 5th round by guessing 48 key bits. Then we check a linear relation between bits in the 4th round, which serves as a filter. A bias for the approximation is $\varepsilon = 2^{-17}$ and we need we need $\varepsilon^{-4} = 2^{68}$ chosen plaintexts to detect the bias. Therefore the time complexity of the attack is $2^{48+68} = 2^{116}$.

5 IMPOSSIBLE DIFFERENTIAL OF ROUND REDUCED SCREAM

An impossible differential path is a differential path which can not occur. Typically we build such a path by the miss-in-the-middle approach, that is showing a contradiction somewhere in the middle of characteristics.

Consider we have a 4-round characteristic of Scream. Each round consists of an S-box followed by an L-box. After each 2 rounds 128-bit key is added. We use a path shown in the figure 1. In the given path as shown in figure 1, each symbol represents a byte. In our notation '00' denotes the zero difference, '$**$' denotes non zero difference and '??' denotes an uncertain difference.

We have selected the given characteristic to get the contradiction in the middle. Here, the conflict will occur after 2 rounds. When we encrypt the plaintext for 2 rounds we get 7^{th} byte is as non-zero while others are uncertain. On the other hand side we decrypt ciphertext for 2 rounds and get 7^{th} byte as inactive, therefore it will lead to contradiction.

Table 5: 4-round impossible differential path.

00 00 00 ** 00 00 00 00 00 00 00 00 00 00 00 00
↓
S-box Layer
↓
00 00 00 ** 00 00 00 00 00 00 00 00 00 00 00 00
↓
L-box Layer
↓
** 00 00 00 00 00 ** ** 00 ** ** 00 ** 00 00 **
↓
S-box Layer
↓
** 00 00 00 00 00 ** ** 00 ** ** 00 ** 00 00 **
↓
L-box Layer
↓
?? ?? ?? ?? ?? ?? ** ?? ?? ?? ?? ?? ?? ?? ?? ??
Contradiction
?? ?? ?? 00 00 ?? 00 00 00 00 ?? 00 00 00 00 ??
↑
S-box Layer
↑
** ** ** 00 00 ** 00 00 00 00 ** 00 00 00 00 **
↑
L-box Layer
↑
00 00 ** 00 00 ** 00 00 00 00 00 00 00 00 00 00
↑
S-box Layer
↑
00 00 80 00 00 80 00 00 00 00 00 00 00 00 00 00
↑
L-box Layer
↑
80 80 00 00 80 00 80 00 80 00 00 00 00 00 80 00

Extracting Key Bits

Here we encrypt many plaintexts to get the required ciphertext which satisfy our characteristic. The number of plaintexts required to encrypt, to get at least one pair of plaintext-ciphertext is $2^{n/2} = 2^{128/2} = 2^{64}$ (where n is the size of state)by using birthday paradox. For all the pairs of plaintext-ciphertext which satisfy the above differential characteristic, we decrypt the ciphertext for 1 round by guessing all possible values of key in 4^{th} round and by applying the inverse L-box followed by the inverse S-box. Here we interchanged the L-Box position with key addition. In case of Scream the L-box is working with row bits and S-box is working with column bits. Therefore for L-box we need 2^{16} combination of target subkeys and again for S-box we need 2^{8} combination of target subkeys, hence we need all the keys to decrypt. To avoid this condition of guessing all keys, we interchange the L-Box position with key addition.

We are interested in those pairs where differences at 3^{rd} and 6^{th} byte after applying inverse S-box in round 4 are same and non-zero, while other differences are zero. This is only possible when S-box inverse in round 4 gives two identical differences. If this is the case, 7^{th} byte before round 3 will be inactive. Therefore, guessed key will lead to a contradiction and we can discard that key. Each time we will halve the remaining candidates for key while always retaining the correct one. The complexity to guess keys and decrypt 2 rounds is 2^{16}. We have calculated from the difference distribution table for S-box and found probability that the transition through the S-box in the 4^{th} round gives two identical differences is approximately 2^{-7}. Therefore the total complexity is $2^{14} \times 2^{64} = 2^{78}$.

6 CONCLUSION

We have analysed Scream with the techniques, which previously have not been applied to this algorithm, that is differential-linear and impossible differential cryptanalysis. This is work in progress towards a comprehensive evaluation of Scream. We think it is essential to analyse these new, promising algorithms with a possibly wide range of cryptanalytic tools and techniques. Our work helps to realize this goal.

REFERENCES

Biham, E. and Shamir, A. (1990). Differential cryptanalysis of des-like cryptosystems. In *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, pages 2–21.

Dobraunig, C., Eichlseder, M., and Mendel, F. (2015). Heuristic tool for linear cryptanalysis with applications to CAESAR candidates. In *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, pages 490–509.

Gandolfi, K., Mourtel, C., and Olivier, F. (2001). Electromagnetic analysis: Concrete results. In *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, number Generators, pages 251–261.

Grosso, V., Leurent, G., Standaert, F., and Varici, K. (2014). Ls-designs: Bitslice encryption for efficient masked software implementations. In *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, pages 18–37.

Grosso, V., Leurent, G., Standaert, F.-X., Varici, K., Journault, A., Durvaux, F., Gaspar, L., and Kerckhof, S. SCREAM. https://competitions.cr.yp.to/round2/screamv3.pdf.

Kocher, P. C., Jaffe, J., and Jun, B. (1999). Differential power analysis. In *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, pages 388–397.

Langford, S. K. and Hellman, M. E. (1994). Differential-linear cryptanalysis. In *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*, pages 17–25.

Leander, G., Minaud, B., and Rønjom, S. (2015). A generic approach to invariant subspace attacks: Cryptanalysis of robin, iscream and zorro. In *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, pages 254–283.

Liskov, M., Rivest, R. L., and Wagner, D. (2011). Tweakable block ciphers. *J. Cryptology*, 24(3):588–613.

Matsui, M. (1993). Linear cryptanalysis method for DES cipher. In *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, pages 386–397.

Todo, Y., Leander, G., and Sasaki, Y. (2016). Nonlinear invariant attack - practical attack on full scream, iscream, and midori64. In *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II*, pages 3–33.