Information Processing Letters 136 (2018) 5–8

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Differential-linear and related key cryptanalysis of round-reduced scream

Ashutosh Dhar Dwivedi [a,*], Paweł Morawiecki [a], Rajani Singh [b], Shalini Dhar [c]

[a] Institute of Computer Science, Polish Academy of Sciences, Warsaw, Poland
[b] Faculty of Mathematics, Informatics, and Mechanics, University of Warsaw, Warsaw, Poland
[c] Sam Higginbottom University of Agriculture, Technology and Sciences, Allahabad, India

ARTICLE INFO

Article history:
Received 23 November 2017
Received in revised form 7 February 2018
Accepted 19 March 2018
Available online 19 March 2018
Communicated by L. Viganò

Keywords:
Block cipher
Linear cryptanalysis
Differential cryptanalysis
Tweakable block cipher
Related key cryptanalysis
Cryptography

ABSTRACT

We have analysed tweakable block cipher Scream which is used by cipher SCREAM, with the techniques linear cryptanalysis, differential cryptanalysis and related key cryptanalysis. Tweakable block cipher Scream is already analysed with linear, differential-linear and impossible differential cryptanalysis in our previous paper. In this paper we extend our work by adding related key attack along with the differential-linear attack.

1. Introduction

Authenticated Encryption (AE) or Authenticated Encryption with Associated Data (AEAD) is a type of encryption that simultaneously provides integrity and confidentiality both, when passing the messages over an insecure channel. It encrypts and authenticates messages using both a secret key (shared by the sender and the receiver) as well as a public number (called a nonce). AE algorithms are often built as various combinations of stream ciphers, block ciphers, hash functions and message-authentication codes.

The great interest and importance of AE have been manifested by the announcement of a new public call for AE algorithms — the CAESAR competition [1]. The contest has started in 2014 and has received worldwide attention. CAESAR candidates are evaluated in terms of robustness, size, security, performance and flexibility. In the first round, 57 algorithms were submitted to CAESAR competition and SCREAM (Side-Channel Resistant Authenticated Encryption with Masking) [4] — the cipher we focus on, is one of the 29 CAESAR round two candidates. However, SCREAM is no longer a candidate to the CAESAR competition in round 3 as it is broken with a new type of attack, called nonlinear invariant attack by Leander et al. [9].

SCREAM is a family of the authenticated encryption algorithms which uses tweakable block cipher Scream introduced in Tweakable Authenticated Encryption (TAE) proposed by Liskov et al. [7]. Compared to conventional block cipher, a tweakable block cipher takes an additional input called *tweak* (Fig. 1). Please note in our paper SCREAM represent Side-Channel Resistant Authenticated Encryption with Masking and Scream is Tweakable Authenticated Encryption used by SCREAM.

2. Related cryptanalysis

Leander et al. [9] presented a paper in Asiacrypt 2016 where they introduced a attack called nonlinear invariant

* Corresponding author.
E-mail address: ashudhar7@gmail.com (A.D. Dwivedi).

https://doi.org/10.1016/j.ipl.2018.03.010
0020-0190/

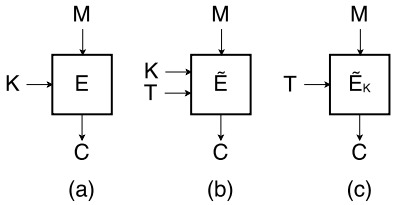

Fig. 1. (a) Standard block cipher encrypts a message M under control of a key K to produce a ciphertext C. (b) Tweakable block cipher encrypts a message M under control of a key K and a "tweak" T to produce a ciphertext C. (c) Here the key K shown inside the box.

attack. In that paper authors showed how to distinguish the full version of tweakable block cipher Scream, i-Scream and Midori64 in a weak key setting. For the authenticated encryption schemes i-SCREAM and SCREAM, the plaintext can be practically recovered only from the ciphertext in the nonce-respecting setting.

In 2017, Dwivedi et al. [2] presented a paper Differential-linear and Impossible Differential Cryptanalysis of Round-reduced Scream, where they analyzed tweakable block cipher Scream with linear, differential-linear and impossible differential cryptanalysis. These techniques previously have not been applied to this algorithm in any other paper.

Leander et al. [6] introduced a generic algorithm to detect invariant subspaces. 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.

3. SCREAM

SCREAM uses tweakable block cipher Scream based on LS-design variant [3] which is denoted as Tweakable LS-designs (TLS-design).

3.1. Tweakable LS-designs

The state is represented as an $s \times l$ matrix, where each element of matrix represents a bit. Therefore the length of the block is $n = s \times l$. The state matrix first row consist of bits from 0 to $l-1$, second row consist of bits from l to $2l-1$, similarly other rows have same length of l bits.

They update a state x of n-bit by iterating N_s steps, each step has N_r rounds. Here row is represented by $x[i,*]$ and a column is represented by $x[*,j]$. The number of rounds per step is fixed as $N_r = 2$. The number of step can vary and it will serve as a parameter of security margins. In the algorithm plaintext is represented by P, TK is represented as the combination of tweak T and master key K.

3.2. The tweakable block cipher Scream

Scream is based on a tweakable LS-design with an 8×16 matrix, i.e. the block length is $8 \times 16 = 128$ bits. Hence the size of the state of Scream is 128-bit, with 8-bit S-boxes and 16-bit L-boxes while the key size is 128-bit denoted by K and 128-bit of tweak denoted by T.

The number of step (each step has 2 round) could vary in Scream depend on security parameters but for related key security, author suggest 10 steps, which is 20 rounds. The round constant $C(r)$ is defined as: $C(r) = 2199 \times r (\text{mod} 216)$. First, the tweak is divided into 64-bit halves, i.e. $T = t_0 \parallel t_1$. Then, every tweakeys is defined as:

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

```
1: x = x ⊕ TK(0)                          ▷ Set plaintext to all-zero vector
2: for 0 < σ ≤ N_s do
3:     for 0 < ρ ≤ N_r do
       r = 2.(σ − 1) + ρ
4:         for 0 ≤ j < l do                ▷ S-box Layer
5:             x[∗, j] = S[x[∗, j]];
6:         end for
       x = x ⊕ C_r;                        ▷ Constant addition
7:         for 0 ≤ i < s do                ▷ L-box Layer
8:             x[i, ∗] = L[x[i, ∗]];
9:         end for
10:    end for
       x = x ⊕ TK(σ)                       ▷ Tweakey addition
11: end for
12: return x
```

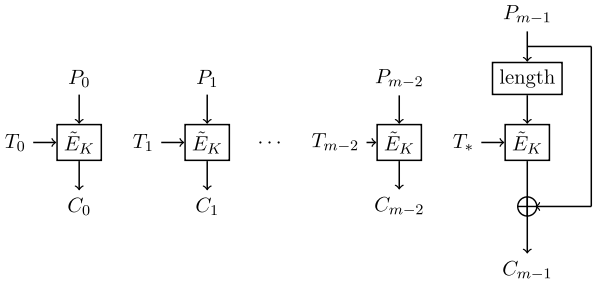

Fig. 2. Encryption of plaintext blocks.

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

$$TK(\sigma = 3i+1) = K \oplus (t_0 \oplus t_1 \parallel t_0) \tag{2}$$

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

3.3. Authenticated encryption SCREAM

SCREAM uses the tweak block cipher Scream in the TAE mode [7]. There are basically three steps in SCREAM: encryption of the plaintext block, associated data processing and tag generation. In our attack we exploits the plaintext block encryption (see Fig. 2).

Using Scream algorithm plaintext values are encrypted to produce the ciphertext values. Here the same value of T_c is used for all blocks, i.e. $T_c = (N||c||00000000)$, where N is the nonce and c is a block counter.

4. Related key-differential-linear cryptanalysis

We tried to extend our previous work on Scream [2] to cover few more round by using related key cryptanalysis along with differential-linear cryptanalysis.

Differential cryptanalysis is the study of how difference in input can affect the resultant difference at the output, while a related key attack is where attacker don't know the keys but he can observe the cipher operation by applying

Table 1
1.5-round differential path with probability 1. (Each column of the state is encoded as two hexadecimal numbers.)

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

several different keys where some mathematical relationship between the keys are known to the attacker. Consider we have two keys $K1$ and $K2$, the relation can be chosen just by XORing a constant $K2 = K1 \oplus C$, where C is known to the adversary. This type of relation allows the adversary to trace the propagation of XOR differences induced by the key difference.

In related-key attack, the information is extracted from the two encryptions under two related keys while related-key differential attack [5] allows the attacker to operate differences in the plaintexts as well as in keys, though the key values are initially unknown.

In case of Scream, which use tweakey scheduling algorithm, consider we have a full control over the tweak T. We tried our experiment for total of 10 rounds which include related key attack of 6 rounds, next 1.5 rounds are differential and then another 2.5 rounds are linear. A total bias is calculated using a formula introduced by Matsui [8].

$$\epsilon_{1,2,3\ldots15} = 2^{n-1} \prod_{i=0}^{i=15} \epsilon_i \tag{4}$$

As a number of plaintext required for the key recovery attack is typically proportional to ϵ^{-4}. For more than 10 rounds we exceed the exhaustive search bound 2^{128} and analysis becomes much less meaningful. After each 2 rounds, a tweak addition is performed. Consider x represent the state after each two rounds. Our equations for 6 rounds of related key are:

$$x = P \oplus T[0] \oplus K \tag{5}$$

$$x = x \oplus T[1] \oplus K \tag{6}$$

$$x = x \oplus T[2] \oplus K \tag{7}$$

To get the best differential-linear characteristic we need a desired output after 6 rounds of related key. Consider we need an output V before the start of differential-linear part. We need such a equation for first 6 round of related key attack where the plaintext difference after each two rounds are 0 for first 4 rounds and become V after 6 rounds. Such equation is possible because we have full control over plaintext P and also tweak T. So, our equations become:

$$x = P \oplus T[0] \oplus K = 0 \tag{8}$$

$$x = x \oplus T[1] \oplus K = 0 \tag{9}$$

$$x = x \oplus T[2] \oplus K = V \tag{10}$$

where $T[0]$, $T[1]$, $T[2]$ represented as:

$$T[0] = (t_0 \parallel t_1) \tag{11}$$

$$T[1] = (t_0 \oplus t_1 \parallel t_0) \tag{12}$$

$$T[2] = (t_1 \parallel t_0 \oplus t_1) \tag{13}$$

If v_0 and v_1 are first half and second half of V then we choose tweak t_0 and t_1 same as v_0 and v_1. Using t_0 and t_1 we can easily calculate $T[0]$, $T[1]$ and $T[2]$. If we set $K = T[1]$, then clearly $T[1] \oplus K = 0$. Then we calculate $TK[0]$ and XOR it with K and set plaintext P accordingly to get 0 difference after XOR operation. By this way we get first 4 round with zero difference of output states after each 2 rounds. Again we calculate $TK[2]$ which will give the desired output. As we mentioned during introduction of tweak $TK[i] = T[i] \oplus K$.

Lets understand this with following values: $V =$ 0000000010000000, here $v_0 =$ 00000000 and $v_1 =$ 10000000, so we choose $t_0 =$ 00000000, $t_1 =$ 10000000 same as v_0 and v_1 respectively. Hence, $T[1] = t_0 \oplus t_1 \| t_0 =$ 1000000000000000. We set the value of $K = T[1] =$ 1000000000000000, by this way $TK[1] = 0$. Using these values of t_0 and t_1 we calculate $T[0] = t_0 \| t_1 =$ 0000000010000000 and $TK[0] = K \oplus T[0] =$ 1000000010000000. Hence, we set the value of $P =$ 1000000010000000. $x \leftarrow P \oplus TK[0] =$ 0000000000000000. Calculated value of $T[2]$ is 1000000010000000. After 4 rounds $x =$ 0000000000000000 and we again add tweak to the state, $x \leftarrow K \oplus T[2] =$ 0000000010000000 which was the desired output.

Once we got the desired output from related key path, we start the differential path for 1.5 round with probability 1. The Table 1 shows differential part of experiment. In the table each symbol represents a byte. In our notation '$**$' denotes non zero difference, '00' denotes the zero difference and '??' denotes an uncertain difference.

Table 2
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

After the second S-box layer in differential path, there are still some bits with known differences. Using these known bits, we build the linear approximation for 2.5 rounds as shown in Table 2. We examine the table for linear approximation of S-box and choose the approximation which has highest bias. Form the table we select the approximation $in_8 = out_8$ (8th input bit of the S-box equals 8th output bit) with bias value 2^{-3}. We use the same bias for all the rounds used in linear approximation. In the below approximation, total active S-boxes are 8 and each has bias value of 2^{-3}. Therefore using the equation 4, total bias for linear approximation will be 2^{-17}.

$$\epsilon_{1,2,3\ldots8} = 2^{8-1} \prod_{i=0}^{i=8} 2^{-3} = 2^{-17} \tag{14}$$

5. Conclusion

The attack uses 6 rounds of related key path, 1.5 rounds of differential path with probability 1 along with 2.5 rounds of linear path with bias value 2^{-17}. By this way we pass total 10 rounds. A bias for the approximation is $\epsilon = 2^{-17}$ and we need $\epsilon^{-4} = 2^{68}$ chosen plaintexts to detect the bias. Therefore the time complexity of the attack is $2^{48+68} = 2^{116}$ as in the attack we peel off the $11th$ round by guessing 48 key bits.

Acknowledgements

Project was financed by Polish National Science Centre, project DEC-2014/15/B/ST6/05130.

References

[1] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness, http://competitions.cr.yp.to/caesar.html.

[2] Ashutosh Dhar Dwivedi, Pawel Morawiecki, Sebastian Wójtowicz, Differential-linear and impossible differential cryptanalysis of round-reduced scream, in: Pierangela Samarati, Mohammad S. Obaidat, Enrique Cabello (Eds.), Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) – Volume 4: SECRYPT, Madrid, Spain, July 24–26, 2017., SciTePress, 2017, pp. 501–506.

[3] Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, Kerem Varici Ls-designs, Bitslice encryption for efficient masked software implementations, in: Carlos Cid, Christian Rechberger (Eds.), Fast Software Encryption – 21st International Workshop, FSE 2014, London, UK, March 3–5, 2014, in: Lect. Notes Comput. Sci., Springer, 2014, pp. 18–37.

[4] Vincent Grosso, Gaetan Leurent, Francois-Xavier Standaert, Kerem Varici, Anthony Journault, Francois Durvaux, Lubos Gaspar, Stephanie Kerckhof, SCREAM, https://competitions.cr.yp.to/round2/screamv3.pdf.

[5] John Kelsey, Bruce Schneier, David A. Wagner, Related-key cryptanalysis of 3-way, biham-des, cast, des-x, newdes, rc2, and TEA, in: Yongfei Han, Tatsuaki Okamoto, Sihan Qing (Eds.), Information and Communication Security, First International Conference, Proceedings, ICICS'97, Beijing, China, November 11–14, 1997, in: Lect. Notes Comput. Sci., Springer, 1997, pp. 233–246.

[6] Gregor Leander, Brice Minaud, Sondre Rønjom, 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, Proceedings, Part I, Sofia, Bulgaria, April 26–30, 2015, 2015, pp. 254–283.

[7] Moses Liskov, Ronald L. Rivest, David Wagner, Tweakable block ciphers, J. Cryptol. 24 (3) (2011) 588–613.

[8] Mitsuru Matsui, Linear cryptanalysis method for DES cipher, in: Tor Helleseth (Ed.), Advances in Cryptology – EUROCRYPT '93, Workshop on the Theory and Application of Cryptographic Techniques, Proceedings, Lofthus, Norway, May 23–27, 1993, in: Lect. Notes Comput. Sci., vol. 765, Springer, 1993, pp. 386–397.

[9] Yosuke Todo, Gregor Leander, Yu Sasaki, 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, Proceedings, Part II, Security, Hanoi, Vietnam, December 4–8, 2016, 2016, pp. 3–33.