Differential Forgery Attack against LAC

Gaëtan Leurent

Differential Forgery Attack against LAC

Gaëtan Leurent

Inria, France
`Gaetan.Leurent@inria.fr`

Abstract. LAC is one of the candidates to the CAESAR competition. In this note we present a differential forgery attack on LAC. We show that some differentials have a probability higher than 2^{-64}, using a collection of characteristics in order to evaluate a lower bound on the probability of a differential. This allows a forgery attack on the full LAC.
This work illustrates the difference between the probability of differentials and characteristics.

1 Introduction

LAC[3] is an authenticated encryption algorithm submitted to the CAESAR competition. LAC uses the same structure as ALE [1]: it is based on a modified block cipher (the G function in LAC is based on LBlock [2]) that leaks part of its state. The main step of the algorithm is to encrypt the current state, and the leaked data is used as a keystream to produce the ciphertext. In addition, plaintext blocks are xored inside the state and the final state is used to produce the tag T. This is depicted in Figure 1.

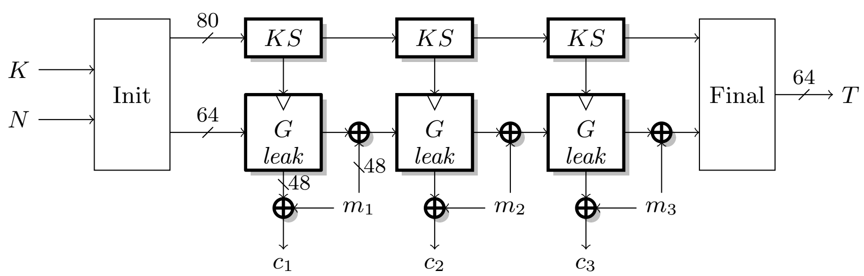

Fig. 1. LAC main structure

In LAC, the main state is 64-bit wide, the key register is 80-bit wide, and the plaintext is divided in blocks of 48 bits. The security goals of LAC against forgery attacks are stated as:

Claim 2 (Integrity for the plaintext)
The security claim of integrity for the plaintext is that any forgery attack with an unused tuple (PMN^*, α^*, c^*, τ^*) has a success probability at most 2^{-64}.

1.1 Description of the attack

Our attack is a differential forgery attack: given the authenticated encryption (C, T) or a message M, we build a cipher-text $(C', T') = (C \oplus \Delta, T)$ that is valid with a probability higher than 2^{-64}.

More precisely, we use a two-block difference $\Delta = (\alpha, \beta)$ so that a difference α is first injected in the state, and we predict the difference β after one evaluation of G in order to cancel it. This will be successful if we can find a differential $\alpha \rightsquigarrow \beta$ in the function G with a probability higher than 2^{-64}.

1.2 Characteristics and differentials

A differential is given by an input difference α and an output difference β. The probability of the differential is the probability than a pair of plaintext with difference α gives a pair of ciphertext with difference β:

$$\Pr[\alpha \rightsquigarrow \beta] = \Pr_{K,x}[E(x \oplus \alpha) = E(x) \oplus \beta].$$

A characteristic is given by an input difference α, the difference α_i after each round, and the output difference β. The probability of the differential $\alpha \rightsquigarrow \beta$ is the sum of the probability of all characteristics with input difference α and output difference β.

The designers of LAC studied its resistance against differential cryptanalysis using truncated characteristics. They show that any characteristic must have at least 35 active S-boxes. Since the best transitions for the S-Box have a probability of 2^{-2}, any characteristic has a probability at most 2^{-70}. However, this does not imply a lower bound for the probability of *differentials*: if many good characteristics contribute to the same differential, the probability can increase significantly.

In this work we give a more accurate estimation of the probability of differentials in the G function of LAC by considering more than one characteristic.

2 Characteristics following the same truncated trail

For a given truncated characteristic D, there exist many ways to instantiate the input/output differences and the intermediate differences. For a given input/output difference (α, β), we consider all the possible intermediate differences following D; this defines a collection of characteristics that all contribute to the same differential. If we can efficiently compute the sum of the probabilities of all those characteristics, this will give a more accurate lower bound of $\Pr[\alpha \rightsquigarrow \beta]$ than by considering a single characteristic.

2.1 Efficient computation

We denote by $\Pr[D : \alpha \rightsquigarrow \beta]$ the probability that a pair with input difference α gives an output difference β, in a way that all the intermediate differences follow the truncated characteristic D. We also denote reduced version of D with only i rounds as D_i.

In order to compute $\Pr[D : \alpha \rightsquigarrow \beta]$ for a given (α, β), we will first compute $\Pr[D_1 : \alpha \rightsquigarrow x]$ for all the differences x following D_1. Then we iteratively build $\Pr[D_i : \alpha \rightsquigarrow x]$ for all x following D_i using the results for D_{i-1}:

$$\Pr[D_i : \alpha \rightsquigarrow x] = \sum_{x'} \Pr\left[D_{i-1} : \alpha \rightsquigarrow x'\right] \times \Pr[x' \rightsquigarrow x]$$

In order to apply this analysis to LAC, we use the truncated characteristic given in Figure 3. We note that this characteristic has at most 6 active nibble at a given round; therefore we have at most 2^{24} probabilities to compute at each step. Moreover, each step has at most 3 active S-Boxes, therefore we have at most 2^9 possible transitions to consider. Using this truncated characteristic, the algorithm can compute $\Pr[D : \alpha \rightsquigarrow x]$ for a fixed α and for all differences x following D with at most $16 \times 2^9 \times 2^{24} = 2^{37}$ simple operations.

After running this computation with all input differences α allowed by the truncated characteristic, we identified 17512 differentials with probability higher than 2^{-64}; the best differential identified by this algorithm has a probability $\Pr[D : \alpha \rightsquigarrow \beta] \approx 2^{-61.52}$. More precisely, the best differentials found are:

$$\Pr\left[\mathtt{0000000000004607} \overset{16}{\rightsquigarrow} \mathtt{0000040000004400}\right] \geq 2^{-61.52}$$
$$\Pr\left[\mathtt{0000000000004607} \overset{16}{\rightsquigarrow} \mathtt{0000060000004400}\right] \geq 2^{-61.52}$$

3 Experimental Verification

In order to check that the algorithm is correct, we ran it with a reduced version of LAC with 8 rounds. We used the second half of the truncated differentials of Figure 3, with 17 active S-boxes. We found that this leads to differential with probability at least $2^{-29.76}$:

$$\Pr\left[\mathtt{0000000000006404} \overset{8}{\rightsquigarrow} \mathtt{0000040000004400}\right] \geq 2^{-29.76}$$
$$\Pr\left[\mathtt{0000000000006404} \overset{8}{\rightsquigarrow} \mathtt{0000060000004400}\right] \geq 2^{-29.76}$$

This has been verified experimentally, and the results match this prediction.

4 Conclusion

Our analysis shows that there exits differentials for the full G function of LAC with probability higher than 2^{-64}. This allows a simple forgery attack with probability higher than 2^{-64} on the full version of LAC, contradicting the security claims. This shows that the security margin of LAC is insufficient.

Our analysis is based on aggregating a collection of characteristics following the same truncated characteristic. While each characteristic has a probability at most 2^{-70}, a collection of characteristic can have a probability as high as $2^{-61.52}$, giving a lower bound on the probability of the corresponding differential.

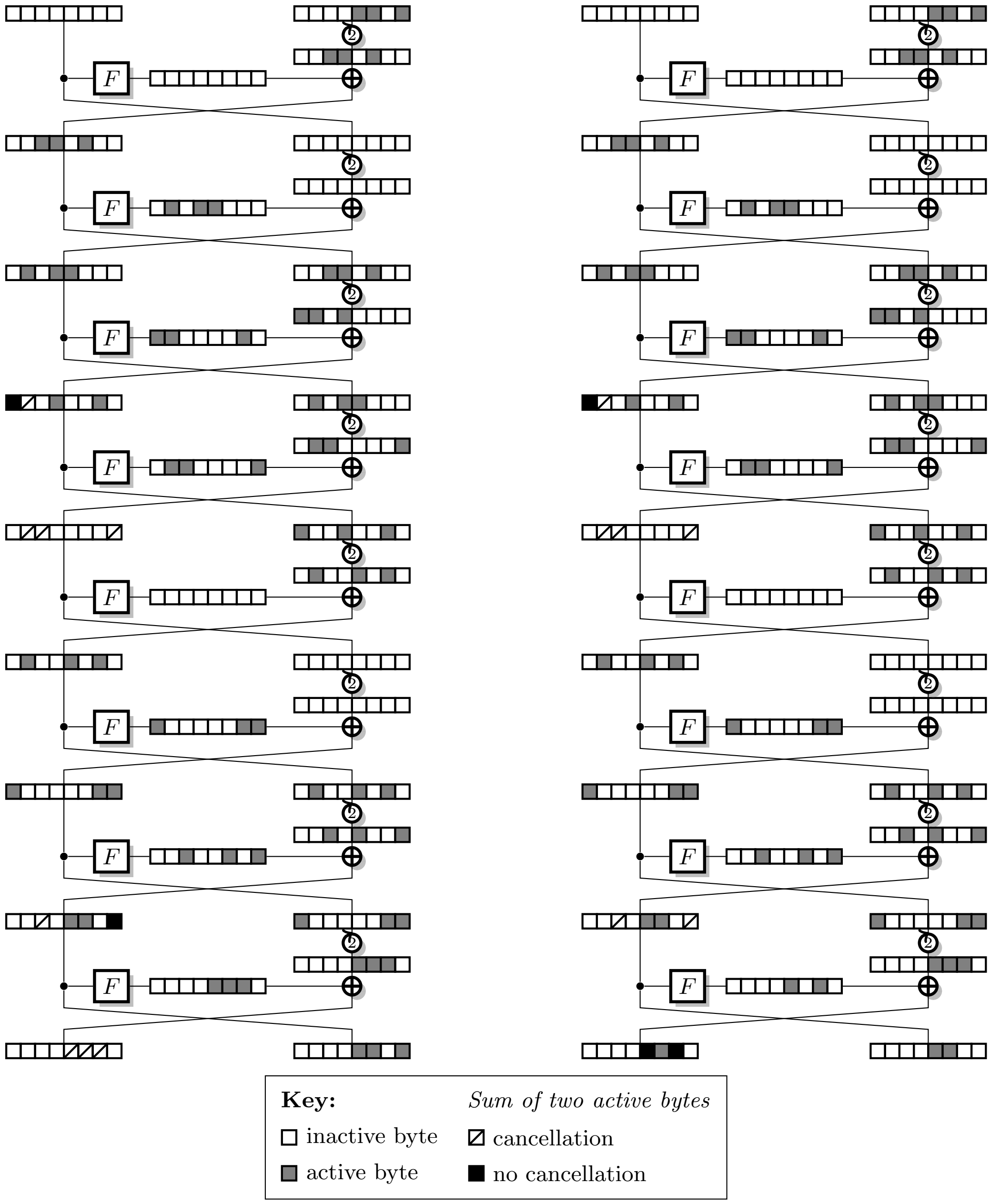

Fig. 2. Truncated characteristic for LAC with 35 active S-boxes.

References

1. Bogdanov, A., Mendel, F., Regazzoni, F., Rijmen, V., Tischhauser, E.: ALE: AES-Based Lightweight Authenticated Encryption. In: FSE (2013)
2. Wu, W., Zhang, L.: LBlock: A Lightweight Block Cipher. In: Lopez, J., Tsudik, G. (eds.) ACNS. Lecture Notes in Computer Science, vol. 6715, pp. 327–344 (2011)
3. Zhang, L., Wu, W., Wang, Y., Wu, S., Zhang, J.: LAC: A Lightweight Authenticated Encryption Cipher. Submission to CAESAR. Available from: `http://competitions.cr.yp.to/round1/lacv1.pdf` (v1) (March 2014)