Practical Forgery on Lilliput-AE

Orr Dunkelman[1], Nathan Keller[2], **Eran Lambooij**[1] and Yu Sasaki[3]

[1]Computer Science Department, University of Haifa, Israel

[2]Department of Mathematics, Bar-Ilan University, Israel

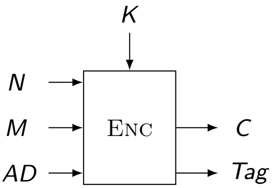
[3]NTT Secure Platform Laboratories, 3-9-11, Midori-cho Musashino-shi, Tokyo 180-8585, Japan

7 November 2019

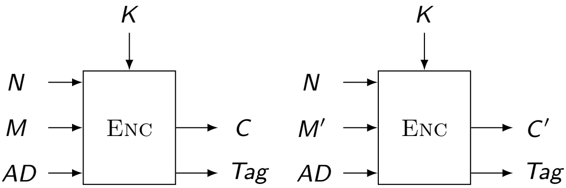
Plan of Tackling

- (Short) recap of Authenticated Encryption.
- Lilliput.
- Probability 1 Related-(Twea)Key differential.
- Attack on Lilliput-AE in the Nonce Misuse mode.
- Conclusion.

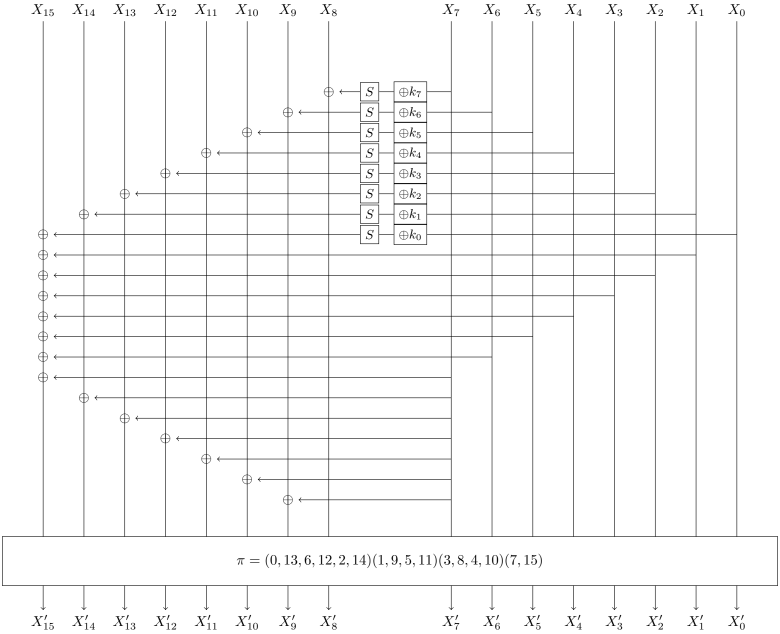
Authenticated encryption + forgery



Authenticated encryption + forgery

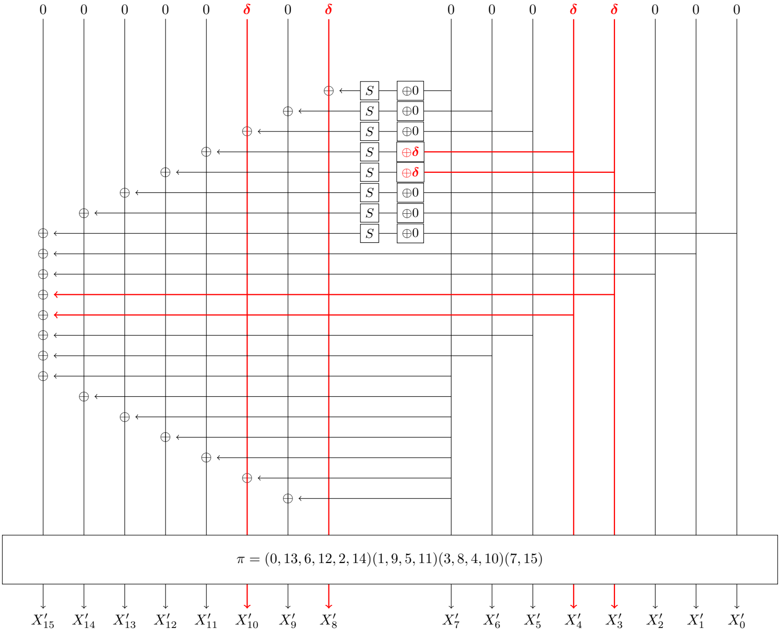


Lilliput



X_{15} X_{14} X_{13} X_{12} X_{11} X_{10} X_9 X_8 X_7 X_6 X_5 X_4 X_3 X_2 X_1 X_0
S
$\oplus k_7$
$\oplus k_6$
$\oplus k_5$
$\oplus k_4$
$\oplus k_3$
$\oplus k_2$
$\oplus k_1$
$\oplus k_0$
$\pi = (0,13,6,12,2,14)(1,9,5,11)(3,8,4,10)(7,15)$
X'_{15} X'_{14} X'_{13} X'_{12} X'_{11} X'_{10} X'_9 X'_8 X'_7 X'_6 X'_5 X'_4 X'_3 X'_2 X'_1 X'_0

Probability 1 Related-(Twea)Key differential

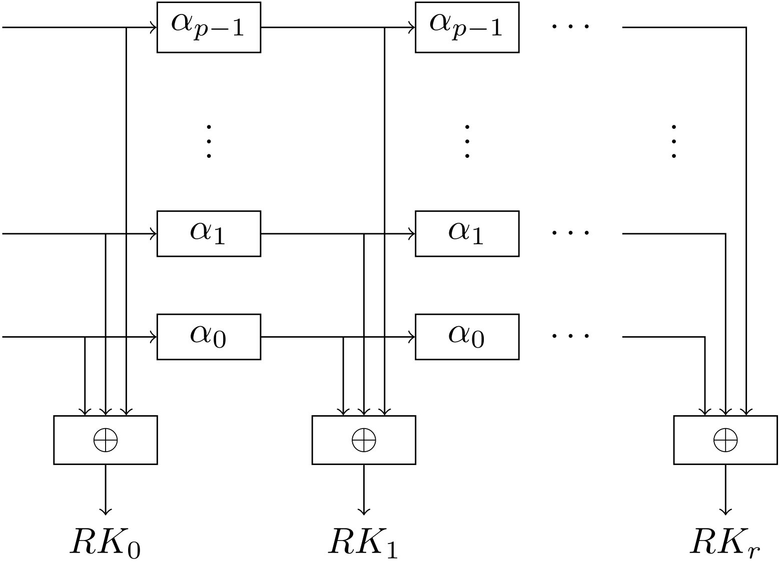


Other differentials

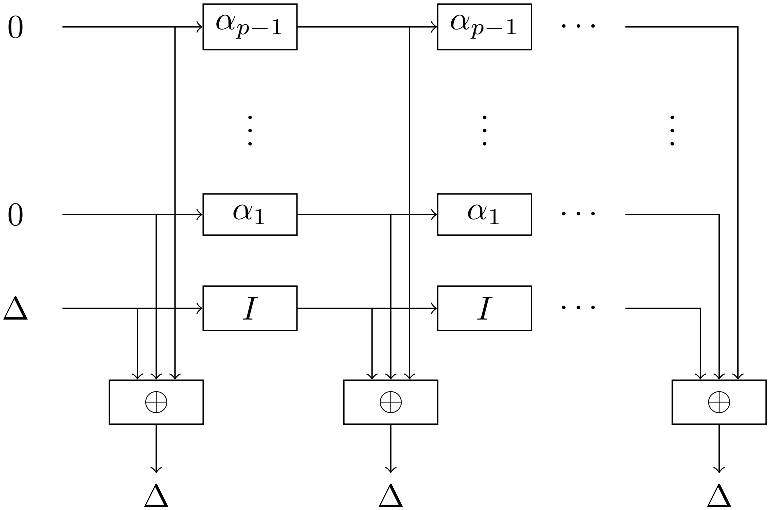
State difference (bytes)	Tweak difference (bytes)
3, 4, 8, 10	3, 4
1, 5, 9, 11	1, 5
0, 2, 6, 12, 13, 14	0, 2, 6
1, 3, 4, 5, 8, 9, 10, 11	1, 3, 4, 5
0, 2, 3, 4, 6, 8, 10, 12, 13, 14	0, 2, 3, 4, 6
0, 1, 2, 5, 6, 9, 11, 12, 13, 14	0, 1, 2, 5, 6
0, 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 14	0, 1, 2, 3, 4, 5, 6

Table: All Related-(Twea)Key differentials possible for the Lilliput round function

Lilliput-AE Key Schedule



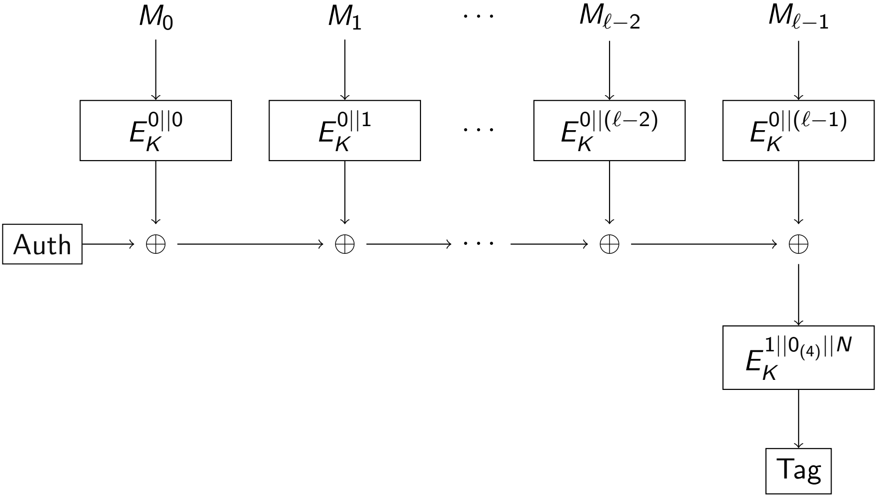
Lilliput-AE Key Schedule Differential



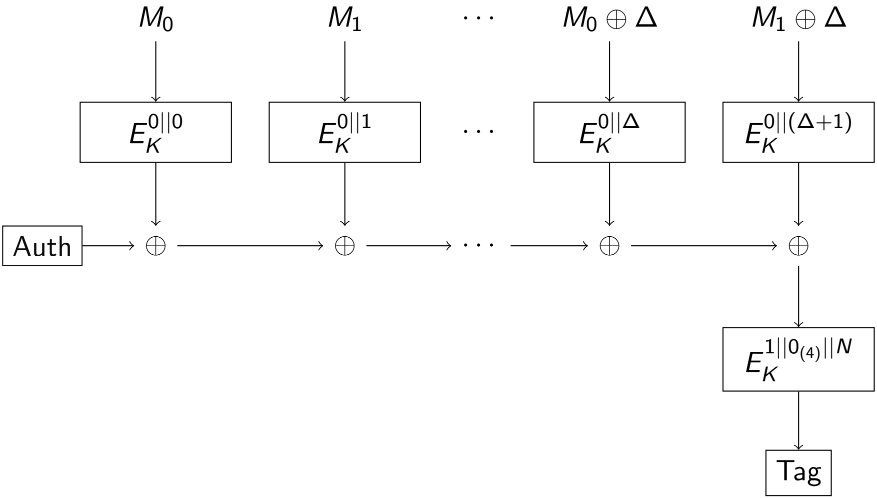
Recap: Observations

- We have a 1 round iterated Related-(Twea)Key differential
- For the differential to work we need the same key difference in every round
- If we introduce a difference in the tweak this difference is inserted every round
- Question: Can we use this to attack the mode?

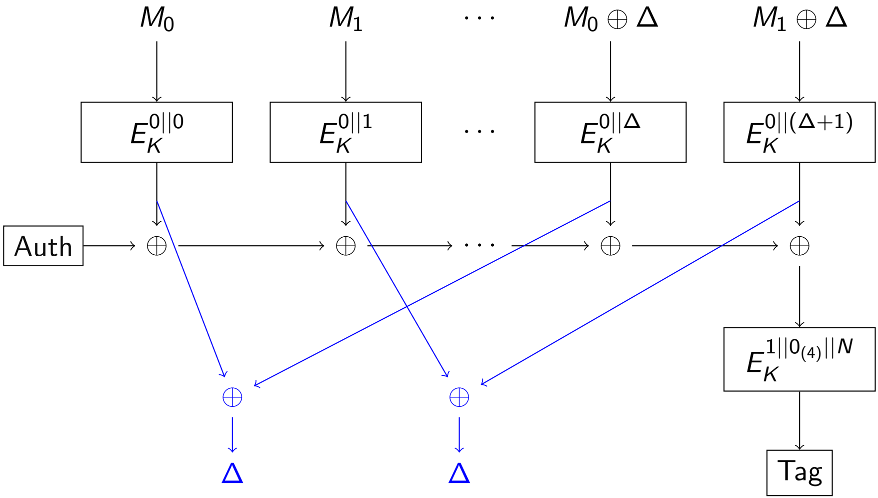
Generating the Tag (Nonce-misuse)



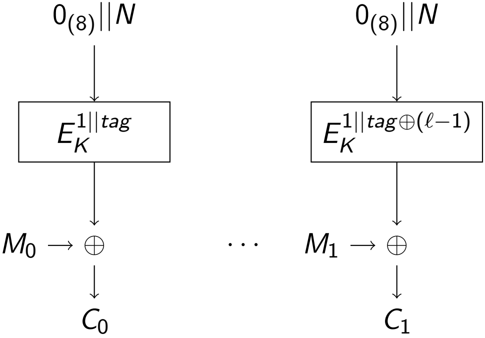
Tag collision (Nonce-misuse)



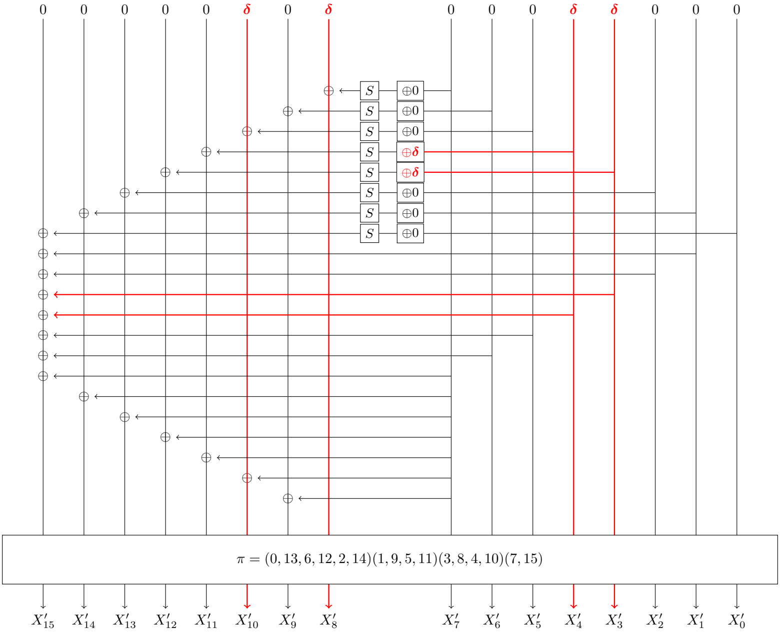
Tag collision (Nonce-misuse)



Encryption (Nonce-misuse)



Probability 1 Related-(Twea)Key differential



Complexity?

- We choose $(0, 0, 0, 01_x, 01_x, 0, 0, 0)$ as the tweak difference.
- The plaintext difference is $(0, 0, 0, 0, 0, 01_x, 0, 01_x||0, 0, 0, 01_x, 01_x, 0, 0, 0)$.
- The tweak reaches this value after $2^{32} + 2^{24} + 1$ blocks in the tag generation.
- Thus we need $2^{32} + 2^{24} + 2$ message blocks to attack the (approx. 64GB).

Why did this work + Proposed Fix

- Lilliput linear layer.
- Tweak does not get updated.
- Interaction between the differential and mode.
- Easy fix: Change α_0 to update the tweak in between rounds.

Conclusion

- We showed a chosen plaintext attack on the nonce misuse mode.
  - With one message of size $2^{32} + 2^{24} + 2$ blocks we can get a tag collision.
  - This allows us to generate the tag and ciphertext for 2^{256} different messages.
- Attacks with known plaintext and in the nonce respecting mode are in the paper.
- Be careful when changing the key schedule of a cipher.
- Related-(Twea)Key differential attacks.

Questions?