Fine-tuning the ISO/IEC Standard LightMAC

Soumya Chattopadhyay[1], Ashwin Jha[2] and Mridul Nandi[1]

[1]Indian Statistical Institute, Kolkata, India
[2]CISPA Helmholtz Center for Information Security, Saarbrücken, Germany

ASIACRYPT 2021

LightMAC: An Introduction

LightMAC is a *parallelizable block-cipher based MAC* first introduced by Luykx et al. in 2016. It has the following features:

- Announced as one of the **ISO/IEC 29192-6:2019** standard lightweight MACs
- Uses two independent block-cipher keys
- Parallel counter-based encoding

LightMAC: A Pictorial Overview

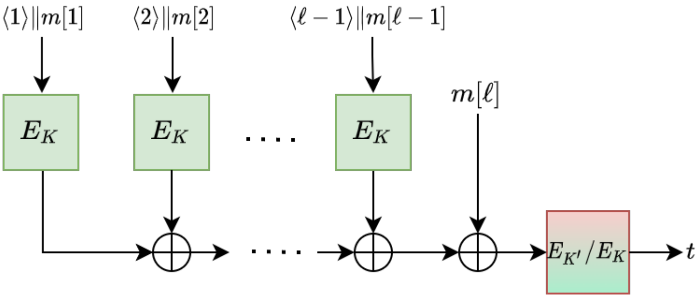


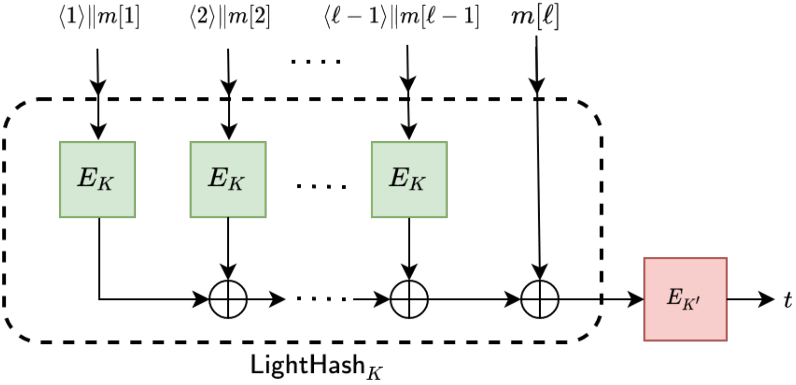
Figure: LightMAC/1k-LightMAC evaluated over an ℓ-block padded message m.

LightMAC: Advantages over other parallelizable MACs

- Simplicity of construction and low overhead.
- Flexibilty: can have compact implementation as well as can exploit parallel structure.

Revisiting the proof schema of LightMAC

PRF security is proved exploiting the *Hash-then-PRP* nature of the construction: $\mathsf{LightMAC}_{K,K'} := E_{K'} \circ \mathsf{LightHash}_K$



Revisiting the proof schema of LightMAC

- Fresh inputs $\Rightarrow$ Random Outputs upto birthday bound (since the keys K, K' are *independent*).
- For 1k-LightMAC the above fact does not hold.
  REASON: Since K, K' are not independent we can not exploit the hash-then-prp structure for randomness here..

Our Contributions

- Security bound of $O(q^2/2^n)$ for 1k-LightMAC, while $(n-s) \leq \ell \leq (n-s)\min\{2^{n/4}, 2^s\}$
- A single-key variant of LightMAC dubbed as LightMAC-ds is proposed and proved to achieve a security bound of $O(q^2/2^n)$ while $\ell \leq (n-s)2^{s-1}$.

Other Results: A Comparative Summary

Mode	#BC Keys	Aux. memory	PRF Bound	Restriction
EMAC	2	0	$q/2^{n/2}$	$\ell \leq n2^{n/4}$
ECBC, FCBC	3	0	$q/2^{n/2}$	$\ell \leq n2^{n/4}$
XCBC	1	$2n$	$q^2\ell/2^n$	$\ell \leq n2^{n/3}$
OMAC	1	n	$q^2\ell/2^n$	$\ell \leq n2^{n/4}$
PMAC	1	n	$q^2\ell/2^n$	-
PMAC3	2	$3n$	$q^2/2^n$	$\ell \leq n2^{n/2}$
LightMAC	2	s	$q^2/2^n$	$\ell \leq (n-s)2^s$
1k-LightMAC	1	s	$q^2/2^n$	$(n-s) \leq \ell \leq (n-s)\min\{2^{n/4}, 2^s\}$
LightMAC-ds	1	s	$q^2/2^n$	$\ell \leq (n-s)2^{s-1}$

1k-LightMAC: Inside View

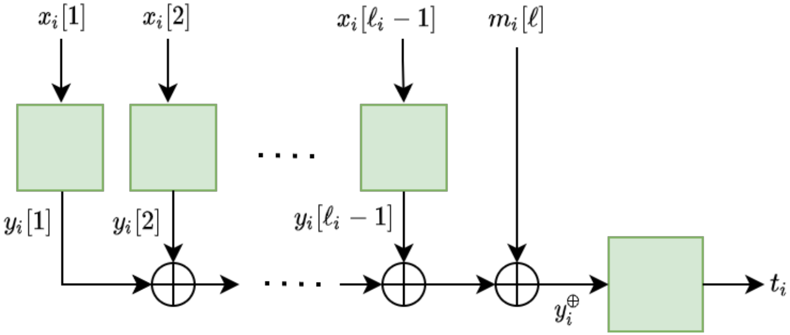


Figure: Input/Output tuples for a message m_i

Bottlenecks for 1k-LightMAC

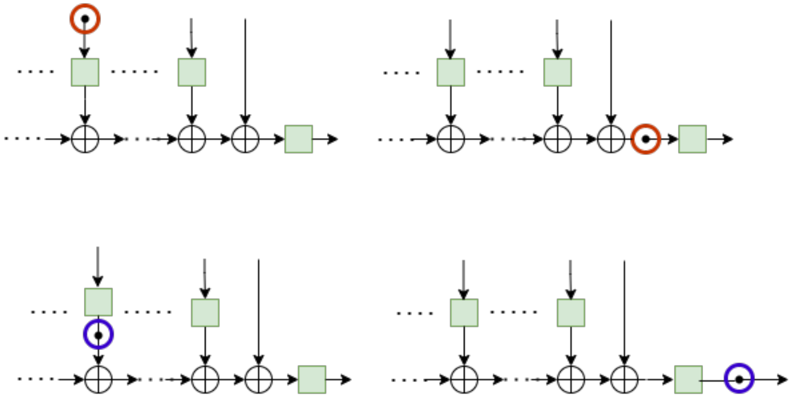


Figure: Red circle denotes Icoll, blue circle denotes Ocoll

Bottlenecks for 1k-LightMAC

Issues with Icoll/Ocoll:

- For LightMAC: No issues with Icoll, Ocoll.
- For 1k-LightMAC: Problem arises if a tuple obtained through ideal oracle is Icoll tuple but *not* Ocoll tuple and vice versa.
- A straightforward approach to avoid these kinds of collision gives $q^2\ell$ terms.

Towards a proof for 1k-LightMAC

H-COEFFICIENT TECHNIQUE will be the general proof environment. Recall that we have to do the following things for applying this technique:

- Define a space of transcripts.
- Define bad and good transcripts.
- Good transcript analysis
- Bad transcript analysis

An overview of the proof for 1k-LightMAC

- **Good trancript analysis:** By choice of our bad events, we get permutation compatibilty between the tuple of all inputs and the tuple of all outputs for a good transcript.

- **Bad trancript analysis:** In this part we employ a novel technique of two-stage sampling due to which we get bounds of $O(q^2/2^n)$ for any bad event.

Reset-sampling: As a way-out for 1k-LightMAC

Given a tuple of messages, we sample Y values in two stages:

- First we sample T and Z values suitably. Z is sampled imitating the internal outputs of the real construction.
- Then Z is reset to Y according to whether it is a full collision tuple or not. (The idea of *full collision tuple* is induced from Icoll)

Reset-sampling: As a way-out for 1k-LightMAC

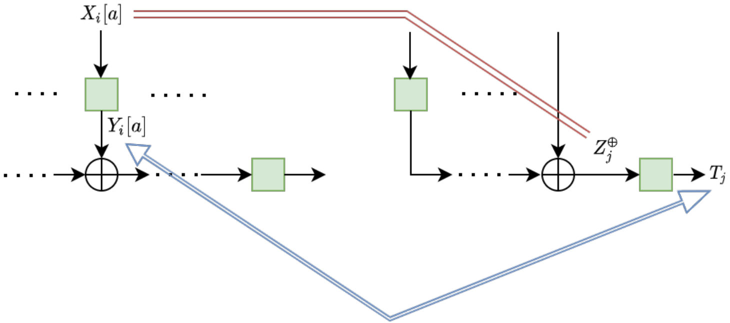
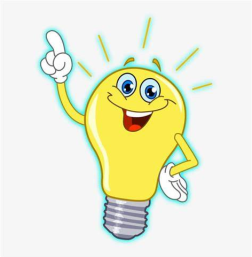


Figure: Resetting Z values to Y values for full collision tuples

Advantage of Reset-Sampling



Intuition behind the approach: Due to two-stage sampling, we might get joint (bad) events which helps to get 2^{2n} in the denominator of the bounds. This compensates for the ℓ factor in the numerator up to a suitable range of ℓ.

Advantage of Reset-Sampling

As an example, consider the following bad event which we get due to resetting:

$$\boxed{badY1 : X_i[a] = Z_j^{\oplus} \wedge X_k[b] = Y_i^{\oplus}}$$

Here we get $q^3\ell^2$ terms in the numerator and 2^{2n} in the denominator. The ratio is ℓ-free for a suitable range of ℓ. Similar treatment is applicable for all other bad events.

1k-LightMAC: Final Result

$$Adv^{prf}_{1k-LightMAC}(\mathcal{A}) \leq \frac{4q^2}{2^n} + \frac{q^3\ell^2_{\max}}{2^{2n}} + \frac{2q^3\ell_{\max}}{2^{2n}} + \frac{q^4\ell^2_{\max}}{2^{3n}} + \frac{2\sigma}{2^n}$$

which is an ℓ-free bound for $(n-s) \leq \ell \leq (n-s)\min\{2^{n/4}, 2^s\}$.

LightMAC-ds: Another single-key variant of LightMAC

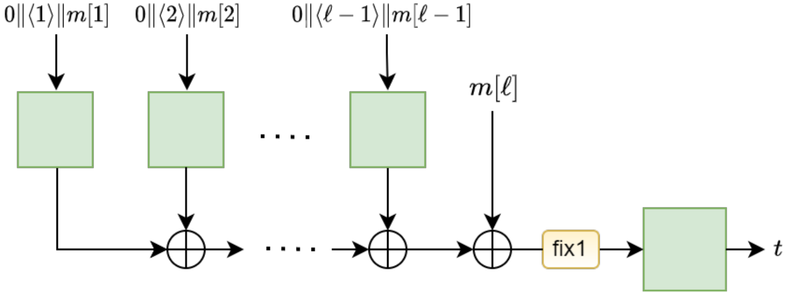


Figure: LightMAC-ds: Here the job of “fix1" is to forcefully fix the msb of the final input string to be 1

LightMAC-ds: Glimpses of Analysis and Security Bound

- No worry to handle Icoll indices!
- Reset-sampling is *not* required here.
- Easier proof than 1k-LightMAC.

$$\boxed{Adv^{prf}_{LightMAC-ds}(\mathcal{A}) \leq \frac{2.5q^2}{2^n}}$$

for $\ell \leq (n-s)2^{s-1}$.

Thank You!