Introducing MGM: Multilinear Galois Mode

draft-smyshlyaev-mgm

Stanislav Smyshlyaev (svs@cryptopro.ru)

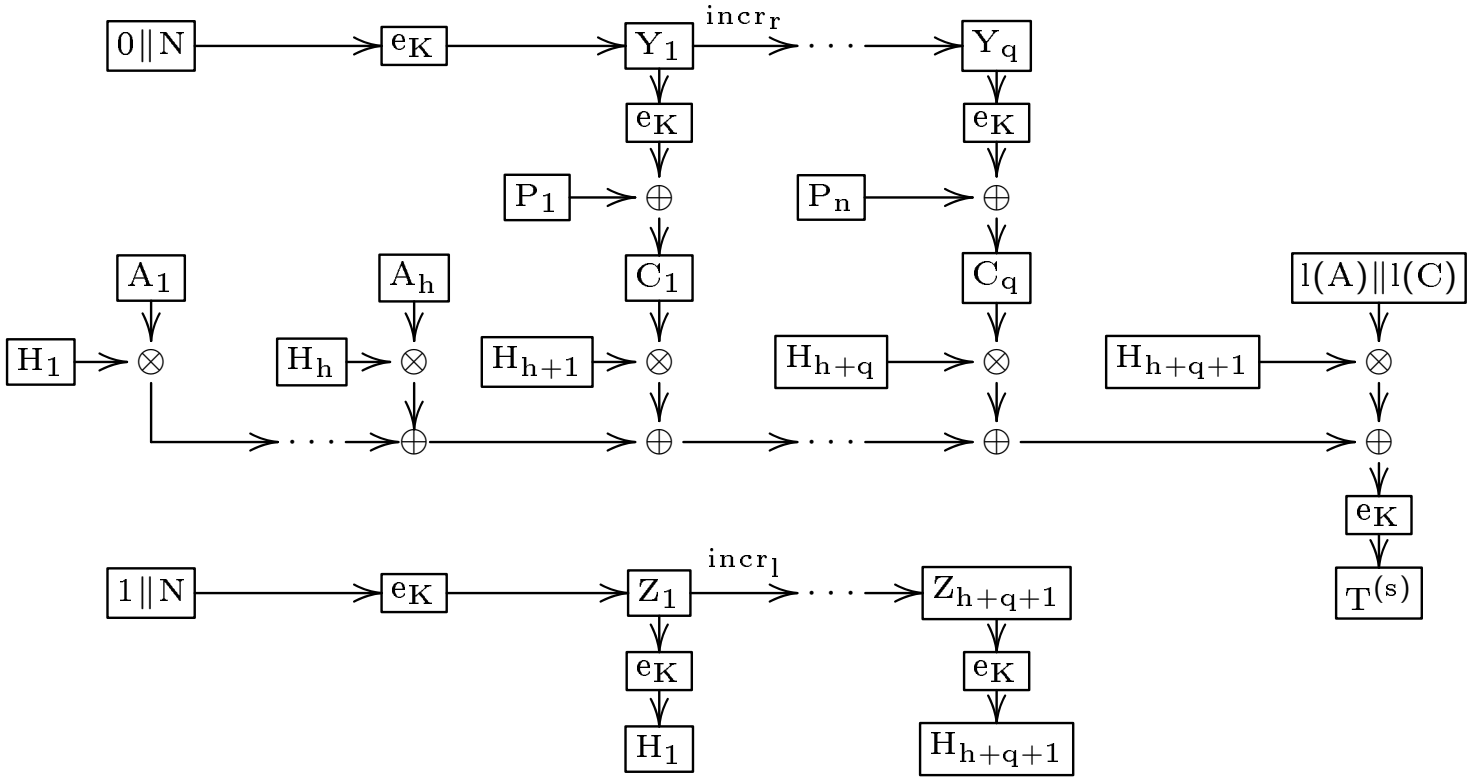
CFRG
IETF 105, July 2019, Montreal

Brief overview

- MGM — an AEAD mode standardized in Russia in 2019.
- Description became available in 2017.
- Motivation for development: need for AEAD mode, security problems of GCM.
- Reasons for not nominating to CAESAR: being too late.

- Don't have any plans for CFRG adoption, just an informative talk.

The construction



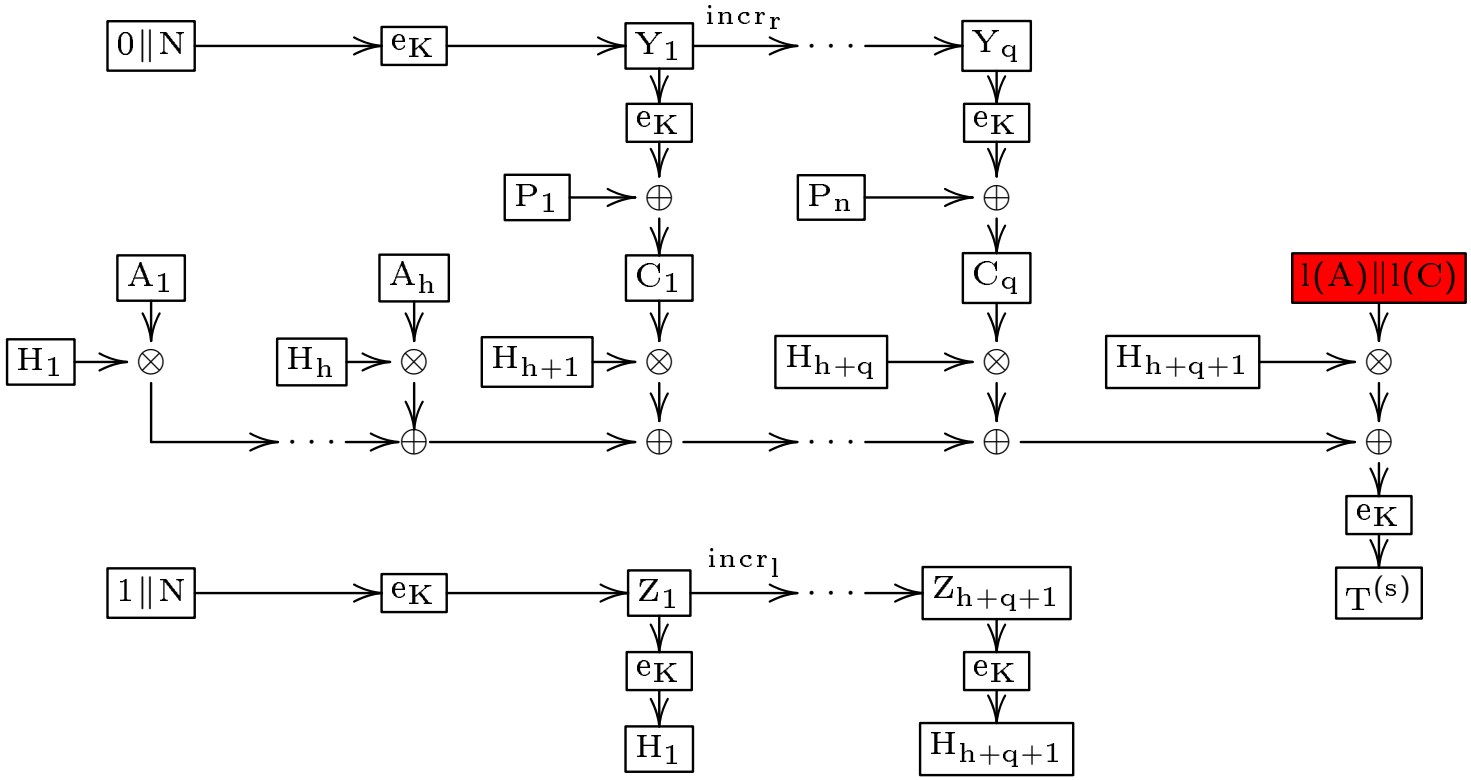
Functional properties

According to NIST 800-38D, GCM has the following properties:

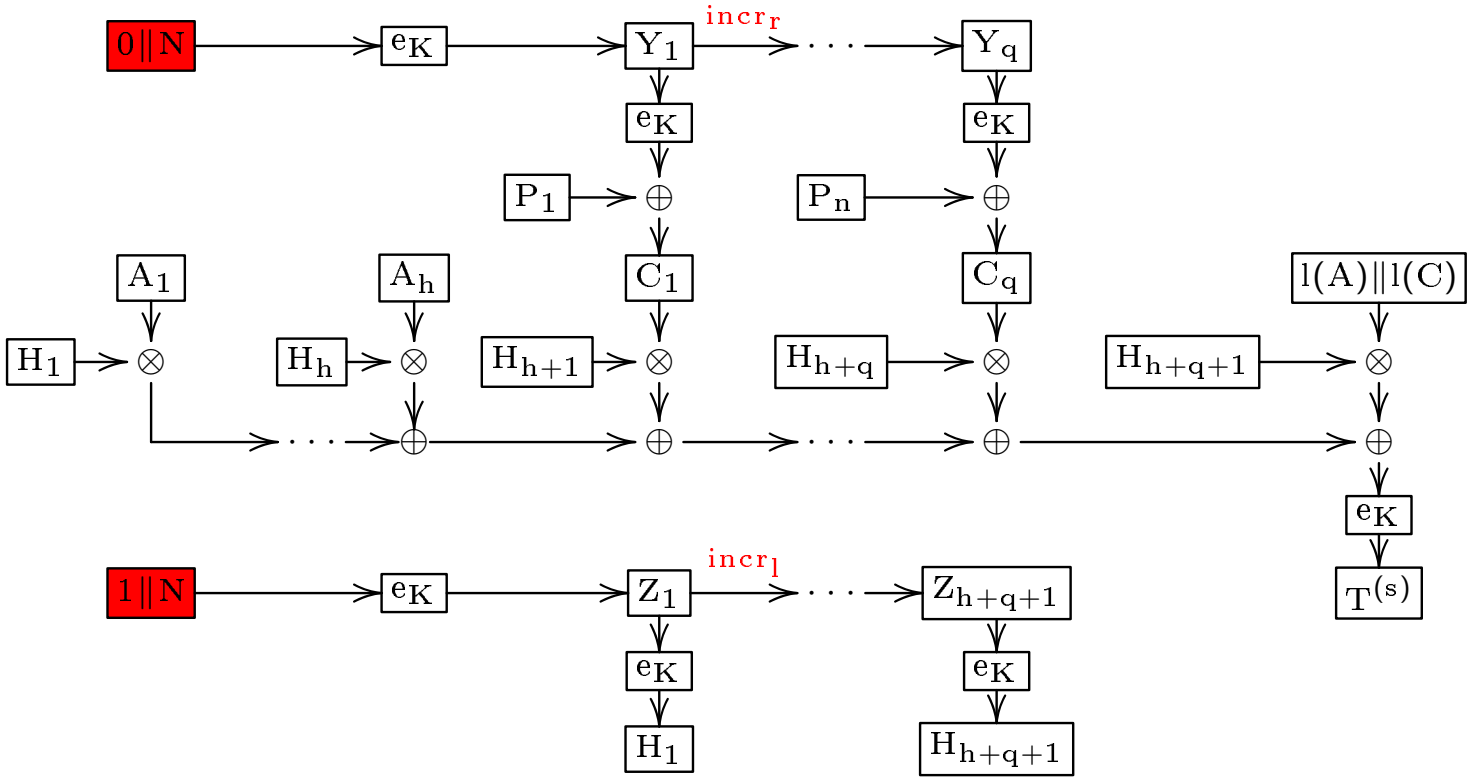
1. Parallelizeable
2. Online
3. Inverse-Free (impementation of E^{-1} is not needed)
4. The authenticity of the protected data can be verified independently from the recovery of the confidential data from its encrypted form
5. If the unique initialization string is predictable, and the length of the confidential data is known, then the block cipher invocations within the GCM encryption mechanism can be pre-computed
6. If some or all of the additional, non-confidential data is fixed, then the corresponding elements of the GCM authentication mechanism can be pre-computed.
7. Only one key is needed.
8. Can be used for MAC only (without encryption).

Same for MGM, excluding 6.

Protection against length extension attacks



Protection against predictable collisions of the counters



Attacks on GCM

Main attacks

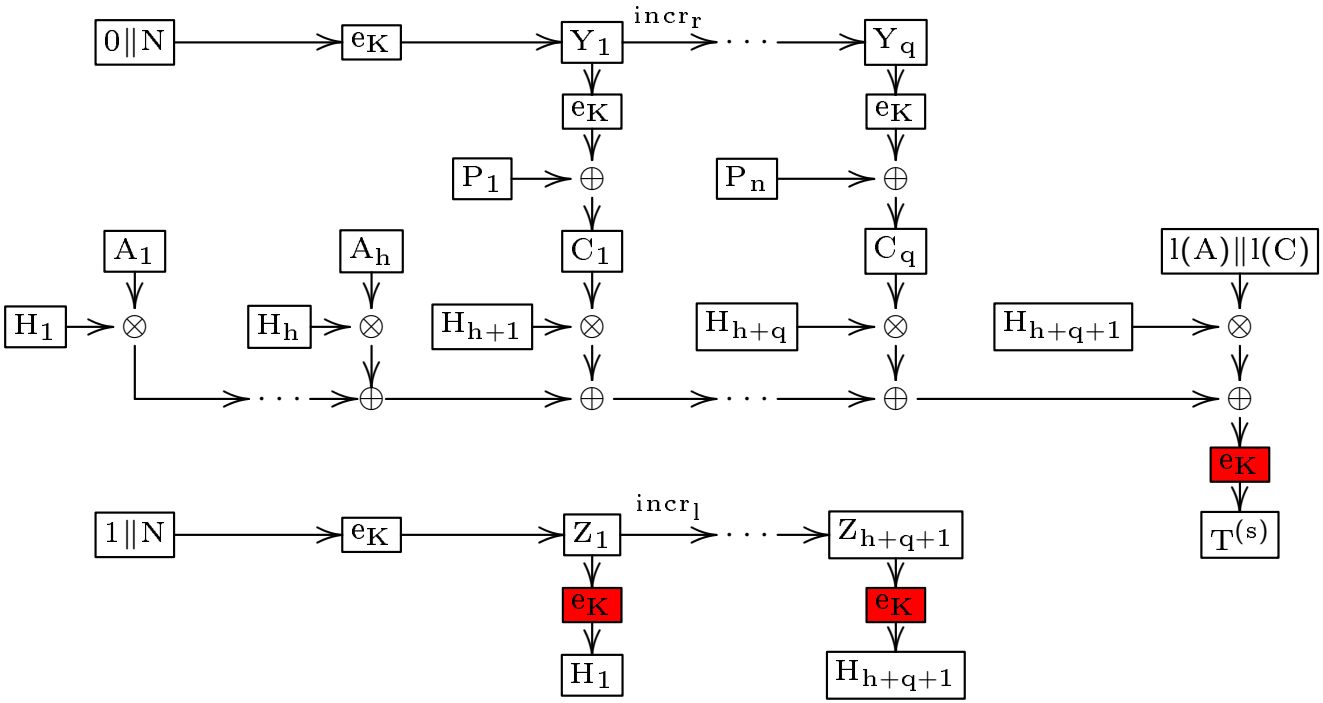
- 2005 – Ferguson, authentication weaknesses;
- 2007 – Joux, “forbidden attack” with repeated IV;
- 2011 – Saarinen, cycling attacks and weak keys.

Other attacks

- 2008 – Handschuh & Preneel’s Key Recovery Attacks;
- 2013 – Procter & Cid’s General Weak-Key Forgery Framework;
- 2015 – Twisted Polynomials and Forgery Attacks.

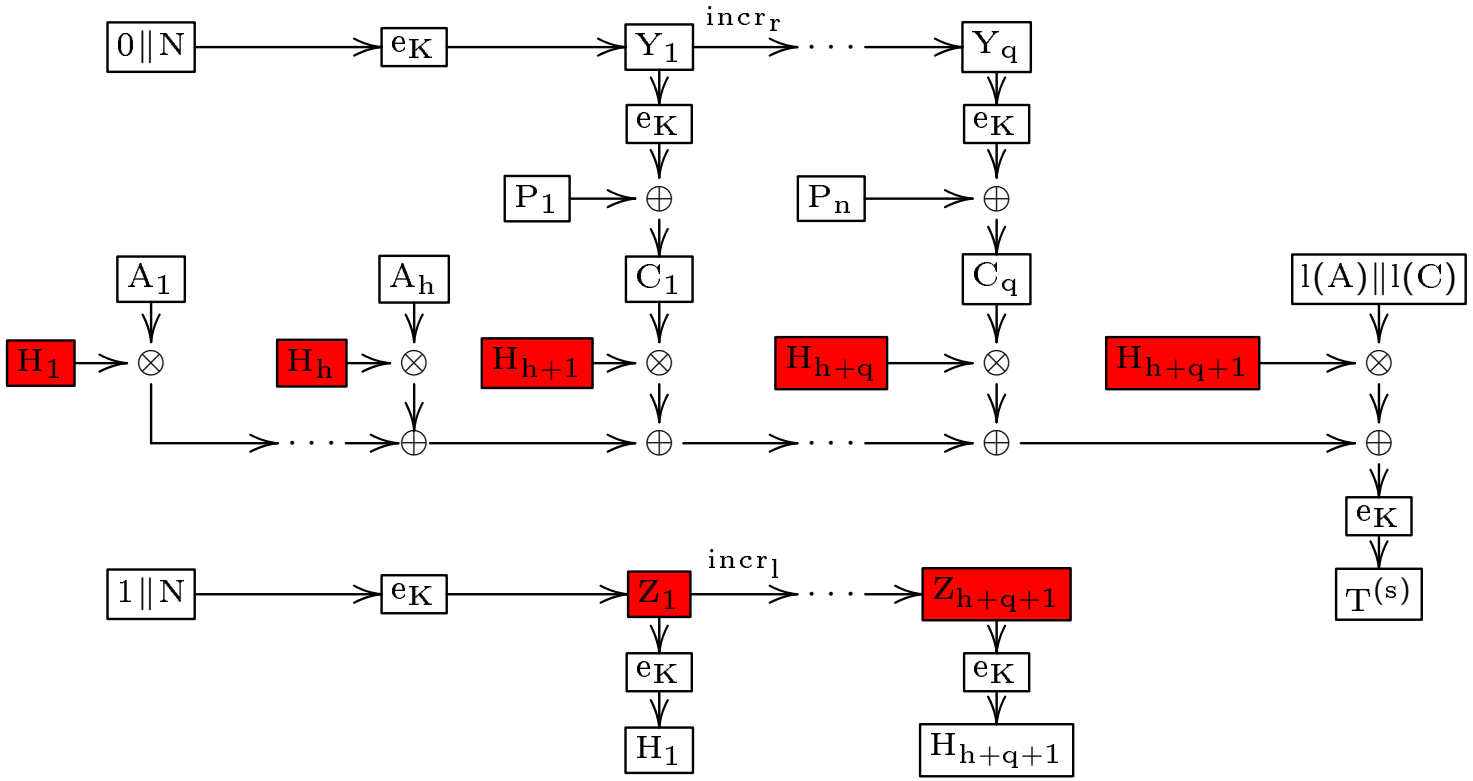
Inapplicability of Ferguson-like attacks

The problem with GCM: the linear structure of GHASH allows to force bits of the result to zero; GCM encrypts the GHASH result by xorring it with a block of key stream, which does not prevent manipulation of the output bits.



Inapplicability of Saarinen-like attacks

The problem with GCM: in certain conditions on a key, ciphertext blocks can be swapped without affecting the tag.



Security bounds

	Confidentiality	Authenticity (one forgery trial)
$\mathrm{GCM}_{[\mathrm{Perm(n)}]}$	$\frac{(\sigma+\mathrm{q})^2}{2^{\mathrm{n}+1}}$	$\frac{\mathrm{l}+1}{2^{\mathrm{s}}} \cdot \delta_{\mathrm{n}}(\sigma+\mathrm{q}+2)$
$\mathrm{MGM}_{[\mathrm{Perm(n)}]}$	$\frac{3(\sigma_{\mathrm{A}}+4\mathrm{q})^2}{2^{\mathrm{n}}}$	$\frac{3(\sigma_{\mathrm{A}}+4\mathrm{q}+\mathrm{l}+3)^2}{2^{\mathrm{n}}} + \frac{2}{2^{\mathrm{s}}}$

$\delta_{\mathrm{n}}(\mathrm{x}) := \frac{1}{(1-\frac{\mathrm{x}}{2^{\mathrm{n}}})^{\mathrm{x}/2}}$

- q is the number of encryption queries
- l is the maximum possible size of one protected message
- σ is the total block length of plaintexts
- σ_{A} is the total block length of plaintexts and associated data
- s is the tag size

„Security of Multilinear Galois Mode (MGM)“, L. Akhmetzyanova et al., Cryptology ePrint Archive: Report 2019/123

Comparison with other AEAD modes

Mode	MGM	GCM	COLM	OCB3	Deoxys-II	ACORN	AEGIS	Ascon	MORUS
Type	BC	BC	BC	BC	BC	SC	Dedic	Sponge	Dedic
Parall. Enc/Dec	+/+	+/+	+/+	+/+	+/+	+/+	+/-	-/-	-/-
Online	+	+	+	+	+	+	+	+	+
Inverse-Free	+	+	-	-	-	+	+	+	+
Incr. AE/AD	-/-	-/-	+/-	-/-	-/-	-/-	-/-	-/-	-/-
Fixed AD Reuse	-	+	+	-	-	-	-	-	-
Intermed. Tags	-	-	+	-	-	-	-	-	-
Security proofs	+	+	-	+	+	-	-	+	-
Precomp.	+	+	-	-	-	+	-	+	+
Calls for enc. function	2m + 4	m + 2	2m + 4	m + 2	2m + 1				

Thank you for your attention!

Questions?

- Materials, questions, comments:
  - svs@cryptopro.ru

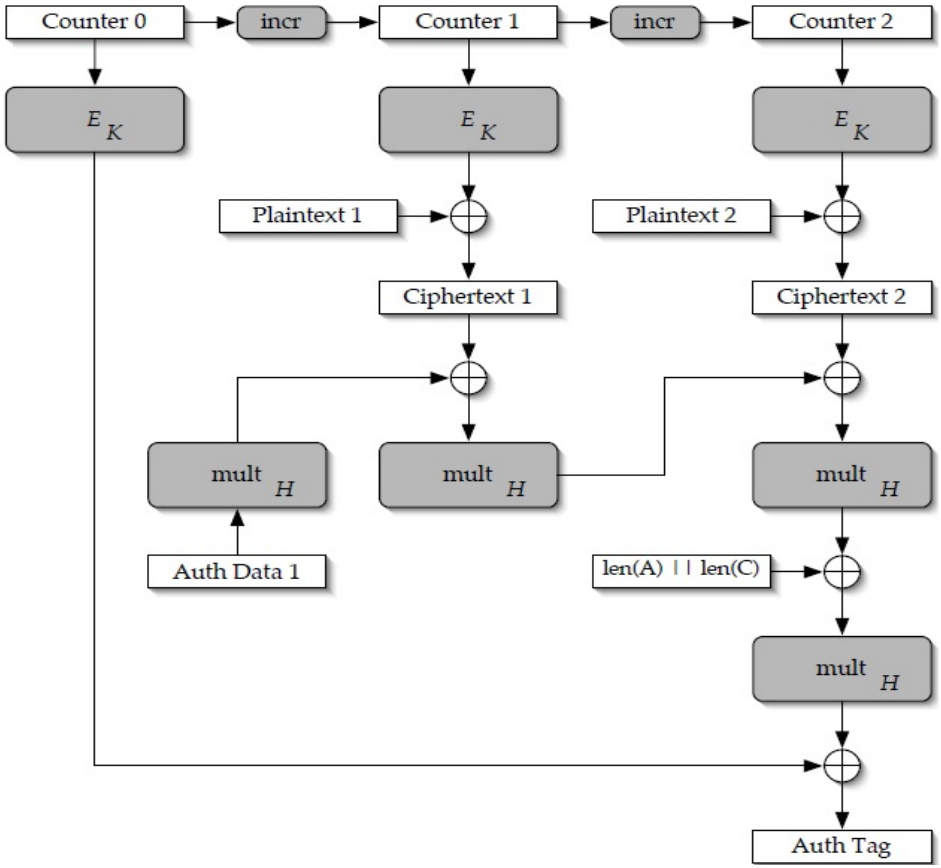
Backup slides

Performance on FPGAs

FPGA implementations: Virtex 6/ Virtex 7

Mode	Throughput (Mbits/s)	Area (LUTs)	TP/A
MORUS	49,421 / 88,576	3,406 / 4,022	14.510 / 22.023
AEGIS	70,927 / 94,208	7,592 / 7,504	9.342 / 12.554
ACORN	11,303 / 11,232	1,224 / 1,234	9.086 / 9.102
Ascon	3,1-5,1 / 4-5,4	1,2-1,5 / 1,5-1,8	2.4-3.2 / 2.6-2.9
GCM	3,239 / 3,223	3,175 / 3,105	1.020 / 1.038
Deoxys-II	2,870 / 3,115	3,162 / 3,297	0.908 / 0.945
MGM	3,490 / 3,840	3,900 / 3,888	0.894 / 0.988
OCB	3,122 / 3,744	4,249 / 4,483	0.735 / 0.835
COLM	3,095 / 3,060	7,718 / 8,131	0.401 / 0.376

Description of GCM



$$Y_0 = \begin{cases} IV\|0^{31}1, & |IV| = 96, \\ GHASH(H, IV), & \text{otherwise.} \end{cases}; \; H = E_K(0); \; \text{mult}_H \text{ — multiplying by H in the field GF}(2^{128})$$

Limits of the modes

For GCM (according to NIST 800-38D 2007)

1. max. length of (P): $\leq 2^{39} - 256 \simeq 64$ GB;
2. max. length of (A): $\leq 2^{64} - 1$;
3. length of IV: $\leq 2^{64} - 1$;
4. MAC sizes: $32, 64, 96, 104, 112, 120, 128$.

For MGM

1. max. length of (P): $\leq 2^{64} - 1$;
2. max. length of (A): $\leq 2^{64} - 1$;
3. length of IV: 127;
4. MAC sizes: from 32 to 128.

Joux, "forbidden attack"

Exploits repeated nonce (which is forbidden).

Obtaining a MAC subkey

- for GCM → malleability for all nonces;
- for MGM → (hypothetically) malleability for the same nonce.

Confidentiality bounds

For any fixed parameters

$$\mathrm{Adv}^{\mathrm{Conf}}_{\mathrm{GCM}} < \mathrm{Adv}^{\mathrm{Conf}}_{\mathrm{MGM}}$$

(due to potential collisions among block cipher inputs in MGM).

However, confidentiality reducing is negligible: for $n = 128$ and q full-size records ($l = 2^{12}$ blocks) in TLS 1.3 we have the following confidentiality bounds

q	GCM	MGM
2^{20}	$\approx 2^{-65}$	$\approx 2^{-62}$
2^{30}	$\approx 2^{-45}$	$\approx 2^{-42}$

Moreover, ciphering nonces in MGM minimizes the number of plaintext/ciphertext pairs of blocks known to an adversary (to resist, e.g., linear and differential cryptanalysis, side-channel attacks).

Authenticity bounds

Consider n = 128, s = 64.

1. TLS 1.3: after processing of recommended number ($q = 2^{24}$) of full-size records ($l = 2^{12}$ blocks)

$$\text{GCM} : \text{Adv}^{\text{Auth}}_{\text{GCM}} \approx 2^{-51}$$

$$\text{MGM} : \text{Adv}^{\text{Auth}}_{\text{MGM}} \approx 2^{-54}$$

2. CMS: after processing of one ($q = 1$) long ($l = 2^{40}$) message

$$\text{GCM} : \text{Adv}^{\text{Auth}}_{\text{GCM}} \approx 2^{-23}$$

$$\text{MGM} : \text{Adv}^{\text{Auth}}_{\text{MGM}} \approx 2^{-44}$$

! MGM is better suited for long messages processing with short tags (due to non-linearity).