Misuse-resistant MGM2 mode

Akhmetzyanova L., Alekseev E., Babueva A., Bozhko A., Smyshlyaev S.

CryptoPro LLC

CRYPTOPRO

CTCrypt'2021

nonce-based AEAD
(**A**uthenticated **E**ncryption with **A**ssociated **D**ata)

$Enc(K, N, A, P) \rightarrow (C, T)$: deterministic encryption algorithm

$Dec(K, N, A, C, T) \rightarrow P\ or\ \perp$: deterministic decryption algorithm

K – key

N – nonce (used only once under single key)

A – associated data (should be authenticated, but not encrypted)

P – plaintext (should be authenticated and encrypted)

C – ciphertext

T – authentication tag

STANDARD SECURITY REQUIREMENTS

confidentiality

integrity

under nonce-respecting CCA (chosen ciphertext attack)

N must be unique

N may be repeated

We need more than the standard properties on practice:

Extend adversary's capabilities:

RUP-resistant AEAD
(release unverified plaintext)

Misuse-resistant AEAD

Leakage-resilient AEAD

Cover new threats:

Nonce-hiding AEAD

Committing AEAD

Provide specific operational properties:

Incremental AEAD

We need more than the standard properties on practice:

Extend adversary's capabilities:

RUP-resistant AEAD
(release unverified plaintext)

Misuse-resistant AEAD

Leakage-resilient AEAD

Cover new threats:

Nonce-hiding AEAD

Committing AEAD

Provide specific operational properties:

Incremental AEAD

Misuse-resistant AEAD

Extends adversary's capabilities: allows to repeat nonces during encryption

N may be repeated

N may be repeated

Why do we need misuse-resistant AEAD?

Case 1: no opportunity to keep internal state or generate random values for providing nonce uniqueness (disk encryption)

Case 2: to get some protection against implementation errors (buffer overflows)

Case 3: to get some protection against active side-channel attacks (fault injection)

Misuse-resistant confidentiality

weak notion

ciphertext of **each query** (N, A, P) **with unique** N is indistinguishable from a «garbage»

«ideal» confidentiality is achieved only for messages that were encrypted correctly

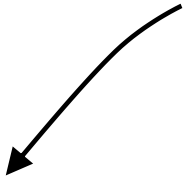
strong notion

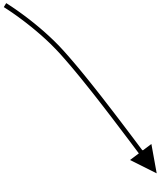
ciphertext of **each unique query** (N, A, P) is indistinguishable from a «garbage»

confidentiality «modulo repetition» is achieved for all messages

SIV, Wide-PRP

Misuse-resistant integrity





weak notion

New ciphertext (N, A, C, T) **only with correctly used N** cannot be forged

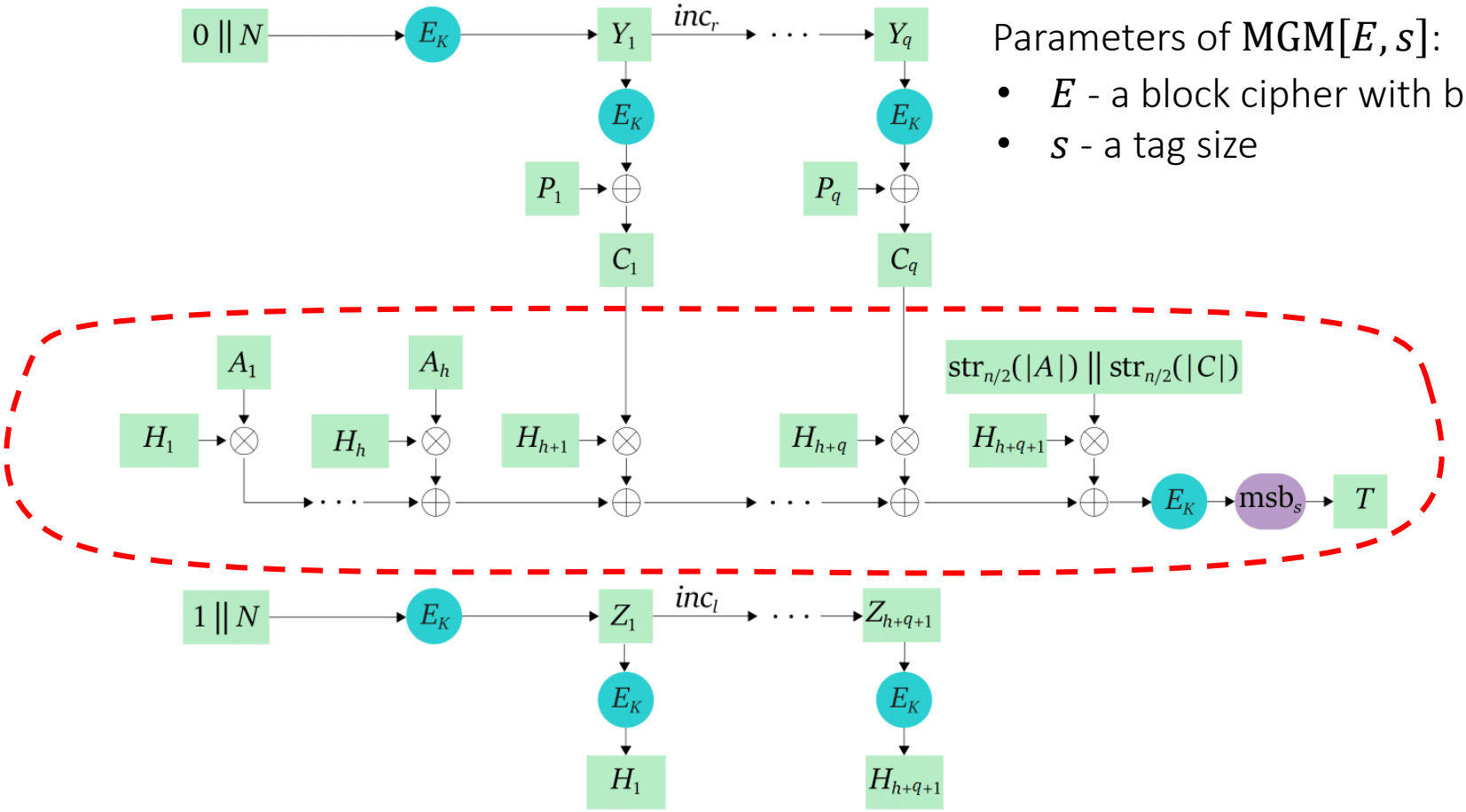
strong notion

New ciphertext (N,A,C,T) **with any N** cannot be forged

MGM – Russian standard AEAD mode

- ✓ **2017** – V. Nozdrunov «Parallel and double block cipher mode of operation (PD-mode) for authenticated encryption», CTCrypt'17.
- ✓ **2018** – First version of RFC draft (draft-smyshlyaev-mgm-20).
- ✓ **2019** – L. Akhmetzyanova, E. Alekseev, G. Karpunin, V. Nozdrunov «Security of Multilinear Galois Mode (MGM)», analysis of MGM in standard models (review phase in Mat. Vopr. Kriptogr.).
- ✓ **2019** – MGM was adopted as a national standard P1323565.1.026-2019.
- ✓ **2019** – A. Kurochkin, D. Fomin «MGM Beyond the Birthday Bound», analysis of MGM in case of (misuse resistant) integrity (birthday-type attack), CTCrypt'19.
- ✓ **2020-2021 –** academic research work on non-standard properties of MGM (led by A. Bondarenko, Academy of Cryptography)

How MGM works?



Parameters of $\mathrm{MGM}[E, s]$:

- E - a block cipher with block size n
- s - a tag size

MGM = double CNT + Multilinear function

Multilinear function – core of MGM

$$\tau = \sum_{i=1}^{h} A_i \otimes H_i \oplus \sum_{i=1}^{q} C_i \otimes H_i \oplus (len \otimes H_{h+q+1})$$

- Good for leakage resilient – each secret coefficient is used just once (in contrast to, e.g., GCM)
- Potentially allows to achieve misuse-resistant integrity (with finalizing enciphering τ)
- Has an incremental property (in case of misuse-resistant integrity with fixed nonce)

Multilinear function – core of MGM

$$\tau = \sum_{i=1}^{h} A_i \otimes H_i \oplus \sum_{i=1}^{q} C_i \otimes H_i \oplus (len \otimes H_{h+q+1})$$

- Good for leakage resilient – each secret coefficient is used just once (in contrast to, e.g., GCM)
- Potentially allows to achieve misuse-resistant integrity (with finalizing enciphering τ)
- Has an incremental property (in case of misuse-resistant integrity with fixed nonce)

… but there are several problems with another part of MGM…

Problem 1

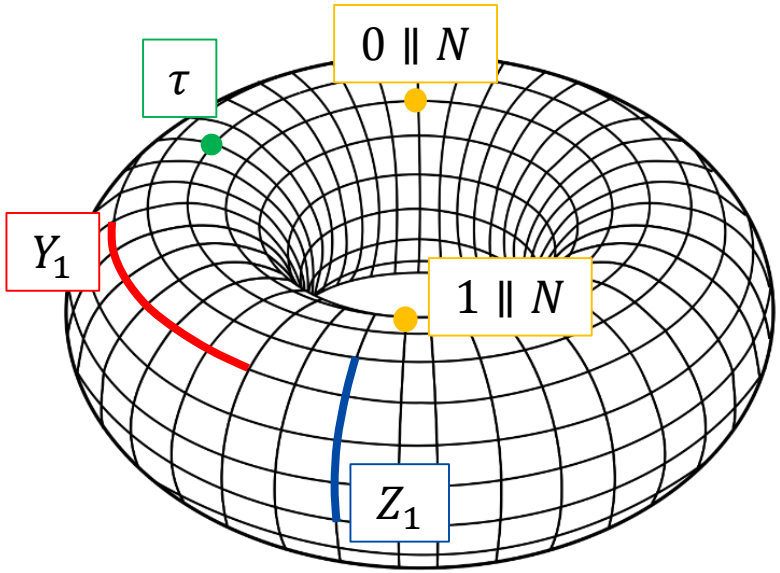
Non-zero probability of collisions between block cipher inputs, used in different “use cases”

⇩

Non-trivial security proofs, which are hard to verify

☹

Extending adversary’s capabilities makes proofs for misuse-resistant integrity more complicated



“Battleship on torus” problem

Problem 2

block cipher inputs are unpredictable

incorporating internal re-keying (like ACPKM) mechanism leads to new collision problems

many «plus one» operations with Y_1 and Z_1, therefore they can leak in case of long messages

can be broken since block cipher inputs must be secret

difficult to achieve leakage resilience

Our contribution

We propose modification of MGM – MGM2:

The same cryptographic core (multilinear function) is used:

all good properties are saved!

double CNT is replaced by double CTR:

solves Problem 1

easier proofs with better bounds for

- misuse-resistant weak confidentiality
- misuse-resistant strong integrity

solves Problem 2

leakage resilience is achievable

- the inputs do not need to be secret
- easy to incorporate re-keying

Our contribution

We propose modification of MGM – MGM2:

The same cryptographic core (multilinear function) is used:

all good properties are saved!

double CNT is replaced by double CTR:

solves Problem 1

easier proofs with better bounds for

- misuse-resistant weak confidentiality
- misuse-resistant strong integrity

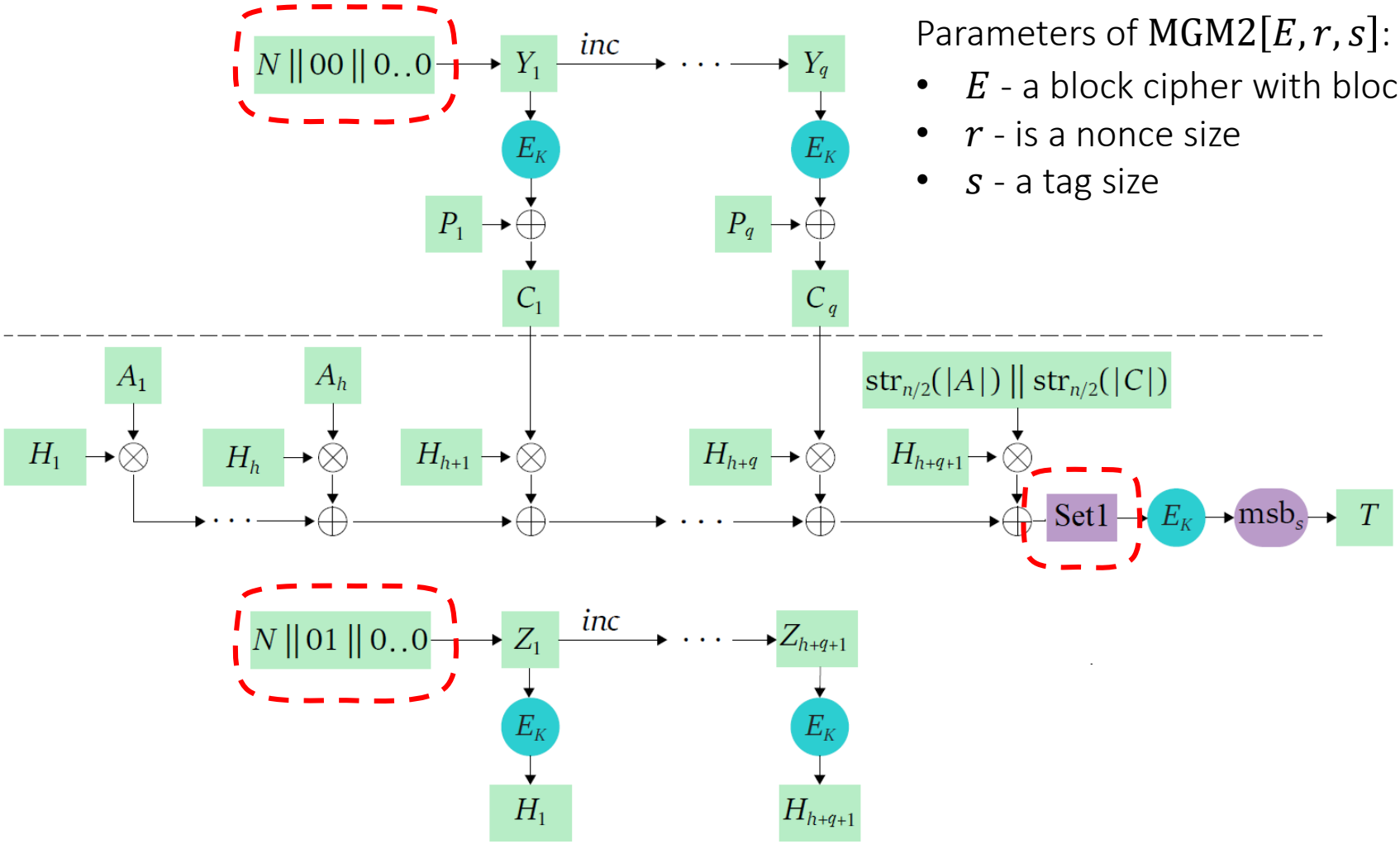
solves Problem 2

leakage resilience is achievable

- the inputs do not need to be secret
- easy to incorporate re-keying

Note: we had not the goal to provide strong misuse-resistant confidentiality (but had in mind a goal to ease providing SIV-construction and proving its security in future)

How MGM2 works?



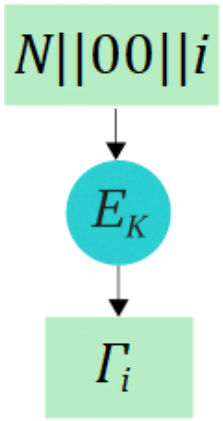
Parameters of $\mathbf{MGM2}[E, r, s]$:

- E - a block cipher with block size n
- r - is a nonce size
- s - a tag size

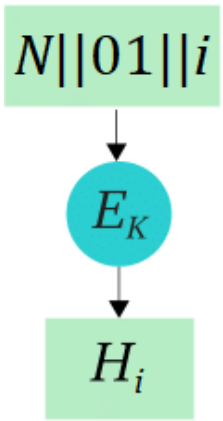
MGM = double CTR + Multilinear function

Differences from MGM

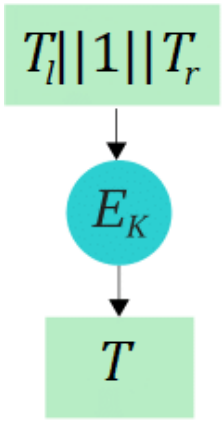
- The way mask values for encryption and the coefficients of the multilinear function are produced – double CNT is replaced by double CTR
- Separation of block cipher inputs, used to generate values for three different use cases by fixing the certain bits of inputs:



mask values



coefficients of the multilinear function



tag values

Security of MGM2

The security of block cipher modes of operation is commonly analyzed under assumption that underlying block cipher is PRP-CPA-secure, i.e. E_K for a random key is computationally indistinguishable from a random permutation $\pi \xleftarrow{U} Perm(n)$.

We provide security bounds directly for the mode with a random permutation $\mathrm{MGM2}[Perm(n), r, s]$ regarding

- ❑ strong misuse-resistant integrity ($MR - int$)
- ❑ weak misuse-resistant confidentiality ($wMR - conf$)

Formal description for these security notions can be found in the paper.

Security of MGM2

We will use the following notations:

σ_A	the total block-length of associated data in all queries
σ_P	the total block-length of plaintexts and ciphertexts in all queries
Q_E	number of queries to the Encrypt oracle
Q_D	number of queries to the Decrypt oracle

Misuse-resistant integrity of MGM2

Theorem 1 (integrity). For any adversary $\mathcal{A}$ breaking strong misuse-resistant integrity of MGM2 the following inequality holds:

$$Adv^{MR-int}_{\mathrm{MGM2}[Perm(n),r,s]}(\mathcal{A}) \le \left(\frac{Q(Q-1)}{2^n} + \frac{Q_D}{2^s}\right)\left(1 - \frac{\sigma - 1}{2^n}\right)^{-\frac{\sigma}{2}},$$

where $Q = Q_E + Q_D$ and $\sigma = 2\sigma_P + \sigma_A + 2Q$.

Misuse-resistant confidentiality of MGM2

Theorem 2 (confidentiality). For any adversary $\mathcal{A}$ breaking weak misuse-resistant confidentiality of MGM2 the following inequality holds:

$$Adv^{wMR-conf}_{\mathrm{MGM2}[Perm(n),r,s]}(\mathcal{A}) \leq \frac{\sigma^2}{2^{n+1}} + \frac{Q_E(Q_E-1)}{2^{n-1}},$$

where $\sigma = 2\sigma_P + \sigma_A + 2Q$.

Proof sketch of the Theorem 1

The proof is carried out in two steps:

1. In the first step we analyze MGM2 with random function: $MGM2[Func(n), r, s]$.

2. In the second step we derive the security bound for MGM2 with random permutation $MGM2[Perm(n), r, s]$ using Bernstein's "analogue" of PRP/PRF switching lemma (Bernstein, D.J. "Stronger Security Bounds for Permutations", 2005).

Theorem 2.3 [Bernstein]. For any distinguisher D^f with oracle $f: \{0,1\}^n \to \{0,1\}^n$, making at most σ queries, the following inequality holds:

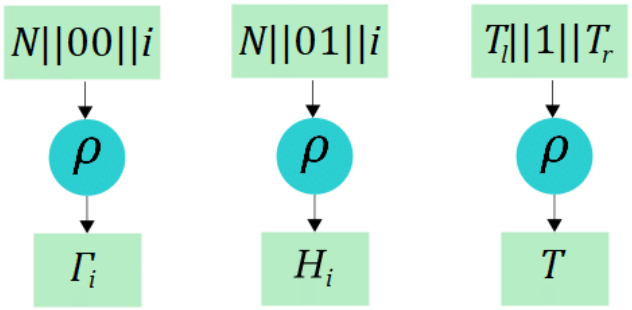
$$\Pr[D^{\pi} \to 1] \leq \Pr[D^{\rho} \to 1] \left(1 - \frac{\sigma - 1}{2^n}\right)^{-\frac{\sigma}{2}},$$

where $\pi \xleftarrow{U} Perm(n)$ and $\rho \xleftarrow{U} Func(n)$.

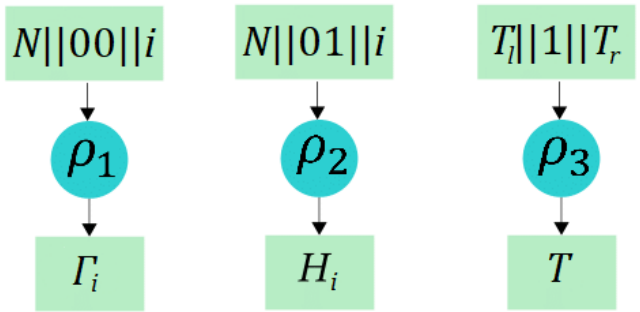
Proof sketch of Theorem 1

Analysis of $\mathrm{MGM2}[Func(n), r, s]$

One random function:



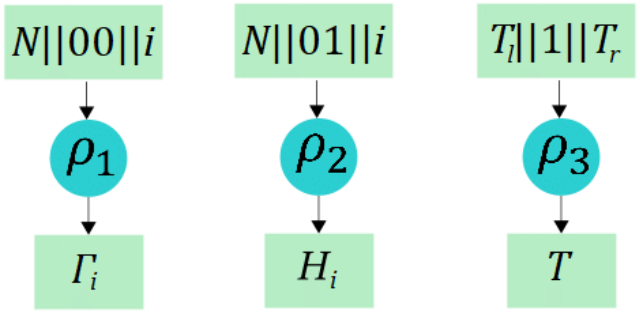
Tree independent random function:



All oracles produce the same distribution on replies for adversary due to the separation of inputs by fixing certain bits

Proof sketch of Theorem 1

Analysis of MGM2 with three random functions



1. We introduce an auxiliary MAC-scheme with nonce called $\mathbf{MGM2MAC}[r,s]$ and based on ρ_2 and ρ_3 and estimate its misuse-resistant UF-CMA security:

$$Adv^{MR-UF-CMA}_{\mathbf{MGM2MAC}[r,s]}(\mathcal{A}) \leq \frac{Q(Q-1)}{2^n} + \frac{Q_D}{2^s}, \text{ where } Q = Q_E + Q_D.$$

2. Then we show that misuse-resistant UF-CMA security of the auxiliary MAC-scheme tightly implies the misuse-resistant integrity of MGM2 with three random functions (ρ_1 , ρ_2 and ρ_3).

MGM vs MGM2

Security bounds for integrity (one-trial forgery):

$$\delta^{int}_{\mathrm{MGM}} \le \frac{\sigma^2}{2^n} + \frac{1}{2^s}$$

$$\delta^{MR-int}_{\mathrm{MGM2}} \le \left(1 - \frac{\sigma - 1}{2^n}\right)^{-\sigma/2} \left(\frac{Q^2}{2^n} + \frac{1}{2^s}\right)$$

$$\sigma = O(\sigma_P + \sigma_A + Q)$$

$n = 128, \sigma \le 2^{n/2}$ (small number Q of long messages):

$$\delta^{int}_{\mathrm{MGM}} \le 1$$ ☹

$$\delta^{MR-int}_{\mathrm{MGM2}} \le 2 \cdot \left(\frac{Q^2}{2^n} + \frac{1}{2^s}\right)$$ ☺

Future work

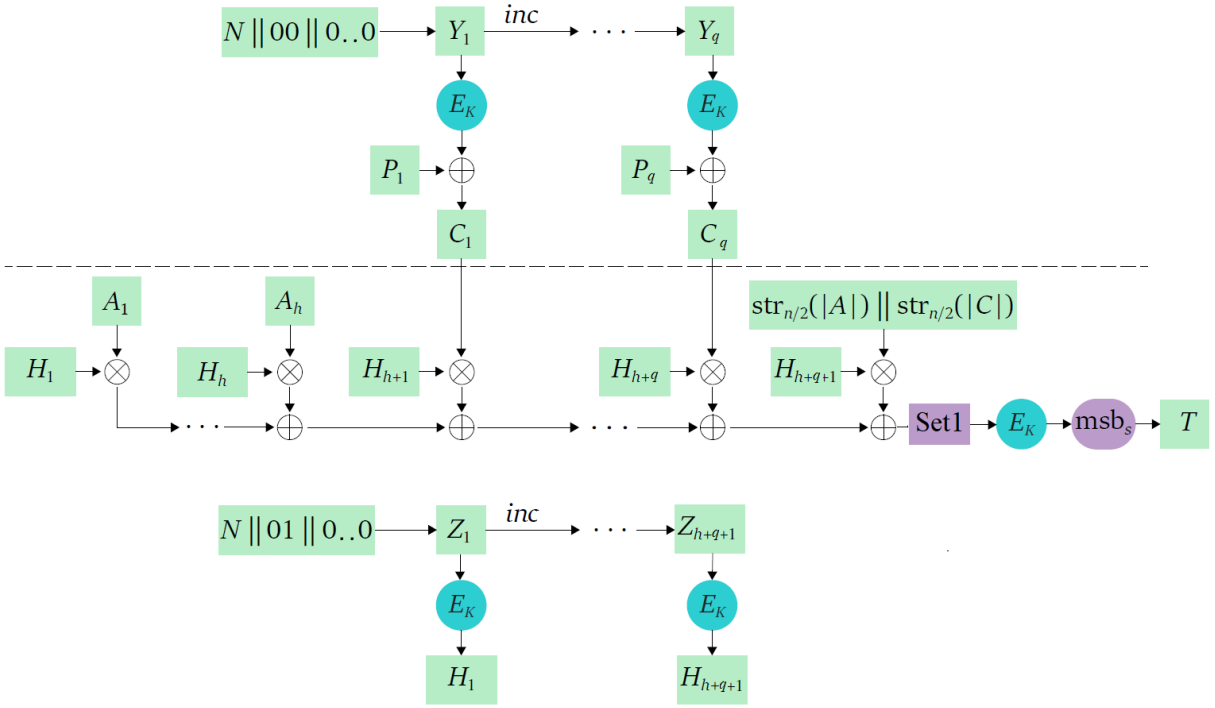
- To analyze RUP-security of MGM2 (needed for CMS)
- To integrate internal re-keying (one bit is reserved for this purpose)
- To propose SIV-construction (to obtain strong misuse-resistant confidentiality)
- To analyze incremental characteristics of MGM2

… and propose an "**MGM family**":

a framework for
constructing an AEAD mode
with necessary security or operational properties

Questions?

☺



Contacts:
lah@cryptopro.ru