# sMGM: parameterizable AEAD-mode

Liliya Akhmetzyanova, Evgeny Alekseev, Alexandra Babueva,
Andrey Bozhko and Stanislav Smyshlyaev

CryptoPro LLC, Moscow, Russia
{lah, alekseev, babueva, bozhko, svs}@cryptopro.ru

**Abstract**

The paper introduces a new AEAD-mode called sMGM (strong Multilinear Galois Mode). The proposed construction can be treated as an extension of the Russian standardized MGM mode and its modification MGM2 mode presented at the CTCrypt'21 conference. The distinctive feature of the new mode is that it provides an interface allowing one to choose specific security properties required for a certain application case. Namely, the mode has additional parameters allowing to switch on/off misuse-resistance or re-keying mechanisms.

The sMGM mode consists of two main «building blocks» that are a CTR-style gamma generation function with incorporated re-keying and a multilinear function that lies in the core of the original MGM mode. Different ways of using these functions lead to achieving different sets of security properties. Such an approach to constructing parameterizable AEAD-mode allows for reducing the code size which can be crucial for constrained devices.

We provide security bounds for the proposed mode. We focus on proving the misuse-resistance of the sMGM mode, since the standard security properties were already analyzed during the development of the original MGM and MGM2 modes.

**Keywords:** MGM, MGM2, AEAD mode, security notion, security bounds, nonce-misuse, misuse-resistant, SIV, re-keying

## 1 Introduction

In this paper we study nonce-based Authenticated Encryption with Associated Data (AEAD) schemes, which aim to provide both integrity and confidentiality of data. The widespread use of AEAD schemes motivates the study of its non-standard security properties, such as misuse-resistance [14], leakage resilience [4] and others [3, 8]. In our work we focus on misuse-resistance and "defense in depth".

Commonly nonce-based AEAD schemes are analyzed in a setting where each new message is encrypted with a previously unused nonce (actually, nonce is a "number used only once"), and the corresponding ciphertext has to be indistinguishable from a random string. However, in some high-level applications nonce uniqueness requirement is hard to fulfill. For example, a nonce can be reused in FDE (Full Disk Encryption) schemes [9], in the case of processes parallelization [5], or as a result of tamper attacks [14]. Hence, the need for misuse-resistant schemes arises. Misuse-resistance is formalized with the MRAE security notion [14], where a ciphertext of each unique message (encrypted with even non-unique nonce) has to be indistinguishable from a random string.

There are several ways to construct a misuse-resistant mode. The first one is wide-PRP constructions with an AEZ mode [13] as an example. Another approach is a SIV (synthetic IV) construction combining arbitrary encryption and tag generation mechanisms in a certain way. The most vivid example of a SIV-based mode is GCM-SIV mode [12]. Both these approaches do not provide high efficiency and have a lack of exploitation properties that can be a deal for constrained devices. As a result, crypto libraries should support various modes and its consumers should be competent enough to select the most efficient mode providing desired security properties. From that our aim is to construct a

single mode that provides a user-friendly interface allowing consumers to simply select the desired security properties, and then the mode would be automatically configured to the optimal way of data processing.

Additionally, we are focusing on increasing the key lifetime which is a critical issue for most applications. This can be achieved by incorporating an internal re-keying technique from [2]. The internal re-keying approach modifies the base mode of operation in such a way that each message is processed starting from the same key, which is changed using a certain key update technique during the processing of the current message. The string consisting of all input cipher blocks processed under the same key is called a section and the key is called a section key. We notice that the internal re-keying also allows us to achieve better security against side channel attacks.

Inspired by ideas used to design the MGM [11, 15] and MGM2 modes [1] and following the aim outlined in the previous paragraphs, we develop a new AEAD mode sMGM (strong MGM). By adjusting certain parameters this mode allows to 1) switch on/off misuse-resistance, which is achieved by applying the SIV construction, and 2) increase the key lifetime using internal re-keying. We design sMGM in such a way that it can be implemented as a single mode and its code size is almost the same as for the conventional modes.

Moreover, sMGM is built with provable security in mind and we provide strict proofs for our security claims in Sections 5.2 and 5.3. In Section 2 we analyze the obtained bounds for several use cases and discuss sMGM design. We notice that the presented proofs contain a new hybrid PRP/PRF switching technique for schemes with re-keying and a new security proof for CTR scheme with re-keying and a random IV in IND-CPA$ [6] model.

## 2 Our contribution

In this section we discuss a new AEAD mode sMGM. The encryption and decryption algorithms of sMGM as well as their domain and range sets are formally defined in Section 4. The sMGM mode is parameterized by the following values:

$$\mathsf{sMGM}\left[\begin{array}{cccc} E, & r, & l_0, l, & siv \\ \text{a block cipher} & \text{a nonce length} & \text{re-keying sections lengths} & \text{misuse-resistance on/off} \end{array}\right]$$

The first and foremost property of sMGM is an optional resistance to nonce misuse, which is achieved by applying SIV-like design [14]. Nonce misuse resistance can be switch on by setting a flag $siv$ to 1. Further for simplicity, we will write sMGMs, when we need to address sMGM with $siv = 1$. In order to support both options and reduce the code size we define two "building blocks", which are CTR-KM and MultTag functions. First one is a CTR-style gamma generation function with incorporated re-keying as in [2]. The second one is a multilinear function used for tag generation, which lies in the core of the original MGM mode [11]. These blocks are used in the Encrypt-then-Mac way, if $siv = 0$, and in Mac-then-Encrypt way (where tag is used as IV during encryption) if $siv = 1$ . The approach is schematically depicted on Figure 1.

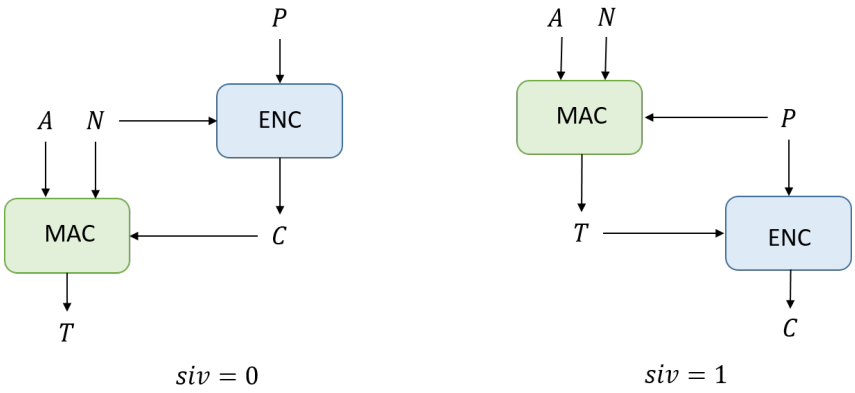


Figure 1: SIV approach

Moreover, sMGM is incorporated with a parameterizable internal re-keying. The major difference between the re-keying in sMGM and other re-keying instantiations lies in a presence of a separate parameter $l_0 \geqslant 0$ for the size of the initial section. The size of subsequent sections is defined by a parameter $l > 0$. The $l_0$ parameter was introduced to control the main key lifetime, since in the sMGM mode the main key is used for processing data more frequently than the subsequent keys. For example, it can be set to 0 and the main key will be used only for generation of subsequent section keys. We notice, that by setting $l_0$ to maximum data length, the re-keying can be switch off completely.

As a result, sMGMs, specially when combined with re-keying, provides a high security level in MRAE model (see Theorem 3) even if a single nonce is used in all queries. Moreover, sMGMs with re-keying has beyond birthday bounds in MRAE-int model (see Theorem 2). In this paper we focus on the security of the misuse resistant version of sMGM, since misuse resistance wasn't previously provided by MGM-like schemes. Security of another sMGM instance (with *siv* flag equal to 0) is somewhat similar to those of MGM2 with re-keying and can be obtained by combining MGM2 security proof from [1] and hybrid technique form GCM-ACPKM proof [2]. We also notice, that the integrity of non-SIV version of sMGM still holds in a nonce misuse setting.

Now we consider two instances of misuse resistant sMGM – with and without re-keying. We consider $E_K$ to be a random permutation with $n = 128$ and $k = 256$. The section sizes for the re-keyed instance are $l_0 = 0$ and $l = 2^6$. In the Table 1 we provide security bounds for these two cases with a growing number $q$ of encryption queries and a *single nonce* value used in all queries. The number of forgery attempts is fixed and equal to 1, the length $m_P$ of plaintexts is bounded by $2^{10}$ blocks or $2^{14}$ bytes (which is the maximum size of TLS 1.3 records) and there is no additional data in all queries. In the table we denote by $\delta_{priv}$ upper bounds for success probabilities of attack on privacy in MRAE model and by $\delta_{int}$ of forgery in MRAE-int model.

## 3 Definitions

Let $|a|$ be the bit length of the string $a \in \{0,1\}^*$. For a bit string $a$ we denote by $|a|_n = \lceil |a|/n \rceil$ the length of the string $a$ in $n$-bit blocks. By $\{0,1\}^{\leqslant s}$ we denote the set of bit strings which length is less or equal to $s$.

For a string $a \in \{0,1\}^*$ and a positive integer $l \leqslant |a|$ let $\mathrm{msb}_\ell(a)$ be the string, consisting of the leftmost $l$ bits of $a$. For nonnegative integers $l$ and $i$ let $\mathrm{str}_l(i)$ be $l$-bit representation of $i$ with the least significant bit on the right, let $\mathrm{int}(M)$ be an integer $i$ such

| $q$ | non re-keyed sMGM | | re-keyed sMGM | |
|---|---|---|---|---|
| | $\delta_{int}$ | $\delta_{priv}$ | $\delta_{int}$ | $\delta_{priv}$ |
| $2^{32}$ | $2^{-62}$ | $2^{-43}$ | $2^{-62}$ | $2^{-49}$ |
| $2^{40}$ | $2^{-46}$ | $2^{-27}$ | $2^{-46}$ | $2^{-33}$ |
| $2^{48}$ | $2^{-30}$ | $2^{-11}$ | $2^{-30}$ | $2^{-17}$ |
| $2^{56}$ | 1 | 1 | $2^{-14}$ | 1 |

Table 1: sMGMs security bounds

that $\mathrm{str}_\ell(i) = M$. For bit strings $a \in \{0,1\}^n$ and $b \in \{0,1\}^n$ we denote by $a \otimes b$ a string which is the result of their multiplication in $GF(2^n)$ (here strings encode polynomials in the standard way). If the value $s$ is chosen from a set $S$ uniformly at random, then we denote $s \xleftarrow{\mathcal{U}} S$. We define a function $\mathsf{Set11}\colon \{0,1\}^n \to \{0,1\}^n$, $\mathsf{Set11}(x) = x$ or $(110\ldots0)$.

For any set $S$, define $Perm(S)$ as the set of all bijective mappings on $S$ (permutations on $S$), and $Func(S)$ as the set of all mappings from $S$ to $S$. A block cipher $E$ with a block size $n$ and a key size $k$ is the permutation family $\big(E_K \in Perm(\{0,1\}^n) \mid K \in \{0,1\}^k\big)$, where $K$ is a key.

# 4 sMGM mode

In this section we define a new AEAD mode – sMGM. The parameters of $\mathsf{sMGM}[E, r, l_0, l, siv]$ are defined in Section 2. For the nonce length the following limits should be observed: $0 \leqslant r \leqslant n - 2 - \lceil \log_2(2\lceil k/n \rceil) \rceil$. The CTR-KM and MultTag functions are defined in Figure 2.

$\mathsf{CTR\text{-}KM}(K, N, IV, f, len)$

$K_0 \leftarrow K$
$t \leftarrow \max(0, \lceil (len - l_0)/l \rceil)$
$st \leftarrow 1,\ end \leftarrow l_0$
**for** $j = 0 \ldots t$ **do**:
  **for** $i = st \ldots end$ **do**:
    $X_i \leftarrow E_{K_j}(0 \| f \| \mathrm{str}_{n-2}(IV + i - 1))$
  **if** $j \neq t$: $K_{j+1} \leftarrow \mathsf{KM}(K_j, N)$
  $st \leftarrow end + 1$
  $end \leftarrow \min(end + l, len)$
**return** $X_1, \ldots X_{len}$

$\mathsf{KM}(K, N)$

$s \leftarrow \lceil k/n \rceil$
**for** $i = 1 \ldots s$ **do**:
  $K^i \leftarrow E_K(10 \| \mathrm{str}_{n-2}(N + i - 1))$
**return** $\mathrm{msb}_k(K^1 \| K^2 \| \ldots \| K^s)$

$\mathsf{MultTag}(K, \{H_1, \ldots, H_{len}\}, M, len)$

$M_1 \| \ldots \| M_{len} \leftarrow M$
$\tau \leftarrow \mathsf{Set11}\left(\bigoplus_{i=1}^{len} M_i \otimes H_i\right)$
$T \leftarrow E_K(\tau)$
**return** $T$

Figure 2: CTR-KM and MultTag functions

The key, plaintext, associated data, ciphertext and tag sets for $\mathsf{sMGM}[E, r, l_0, l, siv]$ are defined as follows: $\boldsymbol{K} = \{0,1\}^k$, $\boldsymbol{N} = \{0,1\}^r$, $\boldsymbol{A} = \boldsymbol{P} = \boldsymbol{C} = \{0,1\}^{\leqslant n(2^{n-2}-2)}$, $\boldsymbol{T} = \{0,1\}^n$. Moreover, the following condition should be satisfied: $0 < |A| + |P| \leqslant n(2^{n-2} - 2)$. The key generation function $\mathsf{sMGM.Gen}()$ is defined as $K \xleftarrow{\mathcal{U}} \{0,1\}^k$, encryption and decryption algorithms are defined in Figures 3a and 3b respectively.

$\mathsf{sMGM}[E, r, l_0, l, \mathbf{0}].\mathsf{Enc}(K, N, A, P)$

$h \leftarrow |A|_n,\ q \leftarrow |P|_n,\ len \leftarrow h + q + 2, s \leftarrow \lceil k/n \rceil$
$N \leftarrow \mathrm{int}(N \| 0^{n-r-2})$

.....Encryption.....

$\{\Gamma_1, \ldots, \Gamma_q\} \leftarrow \mathsf{CTR\text{-}KM}(K, N + s, N, 1, q)$
$C \leftarrow P \oplus \mathrm{msb}_{|P|}(\Gamma_1 \parallel \ldots \parallel \Gamma_q)$

.....Padding.....

$a \leftarrow n|A|_n - |A|,\ c \leftarrow n|C|_n - |C|$
$M \leftarrow A \| 0^a \| C \| 0^c \| \mathrm{str}_n(|A|) \| \mathrm{str}_n(|C|)$

.....Tag generation.....

$\{H_1, \ldots, H_{len}\} \leftarrow \mathsf{CTR\text{-}KM}(K, N, N, 0, len)$
$T \leftarrow \mathsf{MultTag}(K, \{H_1, \ldots, H_{len}\}, M, len)$
**return** $(C, T)$

$\mathsf{sMGM}[E, r, l_0, l, \mathbf{1}].\mathsf{Enc}(K, N, A, P)$

$h \leftarrow |A|_n,\ q \leftarrow |P|_n,\ len \leftarrow h + q + 2, s \leftarrow \lceil k/n \rceil$
$N \leftarrow \mathrm{int}(N \| 0^{n-r-2})$

.....Padding.....

$a \leftarrow n|A|_n - |A|,\ p \leftarrow n|P|_n - |P|$
$M \leftarrow A \| 0^a \| P \| 0^p \| \mathrm{str}_n(|A|) \| \mathrm{str}_n(|P|)$

.....Tag generation.....

$\{H_1, \ldots, H_{len}\} \leftarrow \mathsf{CTR\text{-}KM}(K, N, N, 0, len)$
$T \leftarrow \mathsf{MultTag}(K, \{H_1, \ldots, H_{len}\}, M, len)$

.....Encryption.....

$IV \leftarrow \mathrm{int}(\mathrm{msb}_{n-2}(T))$
$\{\Gamma_1, \ldots, \Gamma_q\} \leftarrow \mathsf{CTR\text{-}KM}(K, N + s, IV, 1, q)$
$C \leftarrow P \oplus \mathrm{msb}_{|P|}(\Gamma_1 \parallel \ldots \parallel \Gamma_q)$
**return** $(C, T)$

(a) sMGM.Enc algorithm

$\mathsf{sMGM}[E, r, l_0, l, \mathbf{0}].\mathsf{Dec}(K, N, A, C, T)$

$h \leftarrow |A|_n,\ q \leftarrow |C|_n,\ len \leftarrow h + q + 2, s \leftarrow \lceil k/n \rceil$
$N \leftarrow \mathrm{int}(N \| 0^{n-r-2})$

.....Padding.....

$a \leftarrow n|A|_n - |A|,\ c \leftarrow n|C|_n - |C|$
$M \leftarrow A \| 0^a \| C \| 0^c \| \mathrm{str}_n(|A|) \| \mathrm{str}_n(|C|)$

..... Tag verification .....

$\{H_1, \ldots, H_{len}\} \leftarrow \mathsf{CTR\text{-}KM}(K, N, N, 0, len)$
$T' \leftarrow \mathsf{MultTag}(K, \{H_1, \ldots, H_{len}\}, M, len)$
**if** $T' \neq T$: **return** $\perp$

.....Decryption.....

$\{\Gamma_1, \ldots, \Gamma_q\} \leftarrow \mathsf{CTR\text{-}KM}(K, N + s, N, 1, q)$
$P \leftarrow C \oplus \mathrm{msb}_{|C|}(\Gamma_1 \parallel \ldots \parallel \Gamma_q)$
**return** $P$

$\mathsf{sMGM}[E, r, l_0, l, \mathbf{1}].\mathsf{Dec}(K, N, A, C, T)$

$h \leftarrow |A|_n,\ q \leftarrow |C|_n,\ len \leftarrow h + q + 2, s \leftarrow \lceil k/n \rceil$
$N \leftarrow \mathrm{int}(N \| 0^{n-r-2})$

.....Decryption.....

$IV \leftarrow \mathrm{int}(\mathrm{msb}_{n-2}(T))$
$\{\Gamma_1, \ldots, \Gamma_q\} \leftarrow \mathsf{CTR\text{-}KM}(K, N + s, IV, 1, q)$
$P \leftarrow C \oplus \mathrm{msb}_{|C|}(\Gamma_1 \parallel \ldots \parallel \Gamma_q)$

.....Padding.....

$a \leftarrow n|A|_n - |A|,\ p \leftarrow n|P|_n - |P|$
$M \leftarrow A \| 0^a \| P \| 0^p \| \mathrm{str}_n(|A|) \| \mathrm{str}_n(|P|)$

..... Tag verification .....

$\{H_1, \ldots, H_{len}\} \leftarrow \mathsf{CTR\text{-}KM}(K, N, N, 0, len)$
$T' \leftarrow \mathsf{MultTag}(K, \{H_1, \ldots, H_{len}\}, M, len)$
**if** $T' \neq T$: **return** $\perp$
**return** $P$

(b) sMGM.Dec algorithm

Figure 3: sMGM mode

## 5 Security analysis

In this section we provide security analysis of misuse resistant sMGM instance (i.e. $\mathsf{sMGM}[E, r, l_0, l, 1]$) in the corresponding models. There are separate results for integrity formalized by MRAE-int model, and chosen ciphertexts confidentiality formalized by MRAE model.

We will denote by $\mathsf{Adv}^{\text{MRAE-int}}_{\mathsf{AEAD}}(\mathcal{A})$ and $\mathsf{Adv}^{\text{MRAE}}_{\mathsf{AEAD}}(\mathcal{A})$ the advantage of an adversary $\mathcal{A}$ succeeding in breaking the properties of the AEAD mode in MRAE-int and MRAE models respectively. The advantage in the MRAE-int model is the probability that an adversary, which may repeat nonces in its queries, is able to forge a ciphertext that will be accepted as valid. The advantage in the MRAE model is the increase in the probability that an adversary, which may repeat nonces in its queries, is able to successfully distinguish an AEAD ciphertext from the output of an ideal cipher. In the MRAE model the adversary also has access to the *Decrypt* oracle, which in ideal world always return an error. These two models are formally defined in Appendix A.

Standard security notion for block ciphers are PRP-CPA («PseudoRandom Permutation under Chosen Plaintext Attack») and PRF («PseudoRandom Function») [6]. We will denote by $\mathsf{Adv}^{\text{PRP}}_{E}(\mathcal{A})$ and $\mathsf{Adv}^{\text{PRF}}_{E}(\mathcal{A})$ the advantage of an adversary $\mathcal{A}$ succeeding in distinguishing $E_K$ from a random permutation and a random function respectively.

### 5.1 Auxiliary results

In this section we introduce some auxiliary results, which will be used throughout subsequent proofs. We begin with Bernstein's result for switching between random permutation and random function.

**Theorem 1** (Theorem 2.3 [7])**.** *For any distinguisher $\mathcal{D}^f$ with an oracle $f\colon \{0,1\}^n \to \{0,1\}^n$, making at most $q$ queries, the following inequality holds:*

$$\Pr[\mathcal{D}^{\pi} \to 1] \leqslant \Pr[\mathcal{D}^{\rho} \to 1] \cdot \left(1 - \frac{q-1}{2^n}\right)^{-q/2},$$

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

Hereafter we will denote an expression $\left(1 - \frac{q-1}{2^n}\right)^{-q/2}$ by $B_q$. The next statement will allow us to switch between a single random function and a set of independent random functions, when applying them to a number of non-overlapping subsets.

**Statement 1.** *For any finite set $A$, any integer $k \leq |A|$, any subsets $A_1, \ldots, A_k \subseteq A$, such that $A = A_1 \sqcup \ldots \sqcup A_k$, $A_i \cap A_j = \emptyset$ for $i \neq j$, and any distinguisher $\mathcal{D}^f$ with an oracle $f : A \to A$, the following equality holds:*

$$\Pr[\mathcal{D}^{\rho} \to 1] = \Pr\left[\mathcal{D}^{\hat{\rho}} \to 1\right],$$

*where $\rho \xleftarrow{\mathcal{U}} Func(A)$ and $\hat{\rho} = \{\rho_1, \ldots, \rho_k\}, \rho_i \xleftarrow{\mathcal{U}} Func(A), \hat{\rho}(a) = \rho_i(a)$ for $a \in A_i$.*

### 5.2 MRAE integrity of sMGMs

**Theorem 2.** *For any* MRAE-int*-adversary $\mathcal{A}$ for* sMGMs*, making at most $q_E$ queries to the Encrypt oracle and at most $q_D$ queries to the Decrypt oracle, where the block-length of associated data in each query is at most $m_A$, the block-length of plaintexts and ciphertexts*

*in each query is at most $m_P$ and the number of distinct nonce values in all queries is at most $q_N$, there exist* PRP*-adversaries $\mathcal{C}$ and $\mathcal{C}_0$ for block cipher $E$, such that*

$$\mathsf{Adv}^{\text{MRAE-int}}_{\mathsf{sMGM}[E,r,l_0,l,1]}(\mathcal{A}) \leq$$
$$\leq \left(\frac{q(q-1)}{2^{n-1}} + \frac{q_D}{2^n} + q_N t_I \mathsf{Adv}^{\text{PRP}}_E(\mathcal{C})\right) \cdot B^{q_N t_I}_{l+s} \cdot B_{q(2l_0+2s+1)} + \mathsf{Adv}^{\text{PRP}}_E(\mathcal{C}_0),$$

*where $q = q_E + q_D$, $s = \lceil k/n \rceil$ and $t_I = \lceil (m_A + m_P + 2 - l_0)/l \rceil$. Adversary $\mathcal{C}$ makes at most $l + s$ queries to its oracle and $\mathcal{C}_0$ makes at most $q(2l_0 + 2s + 1)$ queries.*

*Proof.* For processing the messages sMGMs uses the same block cipher with distinct key values: master key $K$ and section keys $K_i$ that depend on nonce values. We will consider a block cipher with each distinct key as a separate block cipher. Our foremost goal in the first part of the proof is to replace all block ciphers in sMGMs with random functions. This will allow us to apply Corollary 1 from [1] and obtain the bound. Recall, that we write sMGMs instead of $\mathsf{sMGM}[E, r, l_0, l, 1]$ for simplicity.

Now we proceed with the first step of the proof. At this step we replace the block cipher with a master key $K$ by a random permutation $\pi_0$. Note that the block cipher $E_K$ is used for the initial section processing, first re-keying mechanism and tag generation. We write $\mathsf{sMGMs}[E_K]$ to specify the used block cipher. Let us consider experiments $\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[E_K]}$ and $\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\pi_0]}$. In a straightforward manner we construct such an adversary $\mathcal{C}_0$, that

$$\Pr\left[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[E_K]}(\mathcal{A}) \to 1\right] \leq \Pr\left[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\pi_0]}(\mathcal{A}) \to 1\right] + \mathsf{Adv}^{\text{PRP}}_E(\mathcal{C}_0).$$

The adversary $\mathcal{C}_0$ uses the adversary $\mathcal{A}$ as a black box. It intercepts the queries of the adversary $\mathcal{A}$ and process them by itself using its own oracle instead of calling $E_K$ or $\pi_0$. Therefore, to simulate $q$ queries $\mathcal{C}_0$ makes at most $q(2l_0 + 2s + 1)$ calls to its oracle, where $2l_0$ term defines the number of processed blocks in the initial section during encryption and tag generation steps, $2s$ term defines the number of processed blocks in the re-keying mechanism and $+1$ arises from a call in a tag generation process. The adversary $\mathcal{C}_0$ outputs the same bit as the adversary $\mathcal{A}$.

The next step is to replace the random permutation $\pi_0$ with a random function $\rho_0$. Applying Bernstein's result (Theorem 1), we have

$$\Pr\left[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\pi_0]}(\mathcal{A}) \to 1\right] \leq \Pr\left[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\rho_0]}(\mathcal{A}) \to 1\right] \cdot B_{q(2l_0+2s+1)}.$$

Since all inputs to this random function in the cases of 1) computing values $H_j$ for initial section and computing first intermediate key in the tag generation part; 2) computing values $\Gamma_j$ for initial section and computing first intermediate key in the encryption part; 3) computing the tag are different (because of fixed bits in inputs), using one random function is indistinguishable from using three independent random functions $\rho_I, \rho_C, \rho_t$ for these three cases due to Statement 1.

From this, our aim is to replace every block cipher in the tag generation part of sMGMs with a corresponding random function. We denote the keys appearing within the re-keying during processing the $i$-th, $1 \leqslant i \leqslant q_N$, adversarial query with a new nonce by $K_{(i-1)t_I+1}, K_{(i-1)t_I+2}, \ldots, K_{i \cdot t_I}$, where $t_I$ defines the maximum number of sections. Keys $K_{(i-1)t_I+1}$, are generated using random function $\rho_I$ and, since $\rho_I$ inputs are separated with fixed bits for $H_j$ generation and for the re-keying processing, they can be considered random for every new nonce value (follows from Statement 1). Other keys $K_{j+1}$ are generated as $\mathsf{KM}(K_j, N)$. In a case, when a key is chosen randomly, we will write it with calligraphic font – $\mathcal{K}_j$. We will also write $\mathsf{sMGMs}[\rho_I, E_{\mathcal{K}_1}, E_{K_2}, \ldots, E_{\mathcal{K}_{i \cdot t_I+1}}, E_{K_{i \cdot t_I+2}} \ldots, E_{K_{q_N \cdot t_I}}]$

to specify the block ciphers used in each integrity re-keying section in order of appearance (throughout all queries).

Now let us consider experiments $\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\rho_I,\rho_1,\ldots,\rho_{i-1},E_{\mathcal{K}_i},E_{K_{i+1}},\ldots]}$ and $\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\rho_I,\rho_1,\ldots,\rho_{i-1},\pi_i,E_{K_{i+1}},\ldots]}$. In a straightforward manner we construct such an adversary $\mathcal{C}_i$, that

$$\Pr\Big[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\ldots,\rho_{i-1},E_{\mathcal{K}_i},\ldots]}(\mathcal{A}) \to 1\Big] \leqslant \Pr\Big[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\ldots,\rho_{i-1},\pi_i,\ldots]}(\mathcal{A}) \to 1\Big] + \mathsf{Adv}^{\text{PRP}}_E(\mathcal{C}_i).$$

The adversary $\mathcal{C}_i$ uses the adversary $\mathcal{A}$ as a black box. It intercepts the queries of the adversary $\mathcal{A}$ and process them by itself using its own oracle instead of calling $E_{\mathcal{K}_i}$ or $\pi_i$. Therefore, $\mathcal{C}_i$ makes at most $l+s$ calls to its oracle. It outputs the same bit as $\mathcal{A}$.

Next, we replace the random permutation with a random function, applying Bernstein's result (Theorem 1):

$$\Pr\Big[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\ldots,\rho_{i-1},\pi_i,E_{K_{i+1}},\ldots]}(\mathcal{A}) \to 1\Big] \leq \Pr\Big[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\ldots,\rho_{i-1},\rho_i,E_{K_{i+1}},\ldots]}(\mathcal{A}) \to 1\Big] \cdot B_{l+s},$$

where $\rho_i$ is used both for $H_j$ and $K_{i+1}$ generation. However, since $\rho_i$ inputs are separated with fixed bits for these two cases, we can claim, that the key $K_{i+1}$ is generated randomly and independently from $H_j$ (follows from Statement 1). Thus,

$$\Pr\Big[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\ldots,\rho_i,E_{K_{i+1}},\ldots]}(\mathcal{A}) \to 1\Big] = \Pr\Big[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\ldots,\rho_i,E_{\mathcal{K}_{i+1}},\ldots]}(\mathcal{A}) \to 1\Big].$$

Bringing all together, we have the following inequality:

$$\begin{aligned}\Pr\Big[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\ldots,\rho_{i-1},E_{\mathcal{K}_i},E_{K_{i+1}}\ldots]}(\mathcal{A}) \to 1\Big] \leq \\ \leq \Pr\Big[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\ldots,\rho_{i-1},\rho_i,E_{\mathcal{K}_{i+1}}\ldots]}(\mathcal{A}) \to 1\Big] \cdot B_{l+s} + \mathsf{Adv}^{\text{PRP}}_E(\mathcal{C}_i).\end{aligned}$$

Note that in the case, when $\mathcal{K}_i$ is the key of the last section, the same transition can be applied with small differences in justifications. The randomness of the next key (first intermediate key in the next query processing) is achieved earlier, since it is generated by $\rho_I$ function.

Hence, starting from the experiment $\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\rho_I,E_{\mathcal{K}_1},\ldots]}$ and subsequently applying the described transition $q_N \cdot t_I$ times, we obtain

$$\begin{aligned}\Pr\Big[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\rho_I,E_{\mathcal{K}_1},\ldots]}(\mathcal{A}) \to 1\Big] \leq \\ \leq \Big(\ldots\Big(\Pr\Big[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\rho_I,\rho_1,\ldots,\rho_{q_N\cdot t_I}]}(\mathcal{A}) \to 1\Big] \cdot B_{l+s} + \mathsf{Adv}^{\text{PRP}}_E(\mathcal{C}_{q_N\cdot t_I})\Big) B_{l+s} + \\ + \mathsf{Adv}^{\text{PRP}}_E(\mathcal{C}_{q_N\cdot t_I-1})\Big) B_{l+s} + \ldots + \mathsf{Adv}^{\text{PRP}}_E(\mathcal{C}_2)\Big) B_{l+s} + \mathsf{Adv}^{\text{PRP}}_E(\mathcal{C}_1) = \\ = \Pr\Big[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\rho_I,\rho_1,\ldots,\rho_{q_N\cdot t_I}]}(\mathcal{A}) \to 1\Big] \cdot B^{q_N t_I}_{l+s} + \sum_{i=1}^{q_N\cdot t_I} \mathsf{Adv}^{\text{PRP}}_E(\mathcal{C}_i) \cdot B^{i-1}_{l+s}. \quad (1)\end{aligned}$$

It is easy to see, that in the experiment $\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\rho_I,\rho_1,\ldots,\rho_{q_N\cdot t_I}]}$ intermediate keys for tag generation process are produced, but not used — random functions, used to produce coefficients $H_j$, are selected independently from them. From here, we can consider an experiment, where intermediate keys are not generated. Moreover, since the inputs to the functions $\rho_I, \ldots, \rho_{q_N\cdot t_I}$ do not intersect (for repeating nonces we just reuse previously

computed coefficients $H_j$), due to Statement 1, we can unite them under a single random function $\rho_h$. Hence,

$$\Pr\Big[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\rho_I,\rho_1,\ldots,\rho_{q_N\cdot t_I}]}(\mathcal{A}) \to 1\Big] = \Pr\big[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\rho_h]}(\mathcal{A}) \to 1\big]$$

The next step is to proceed only with the tag generation part of $\mathsf{sMGMs}[\rho_h]$. For this let us introduce an auxiliary MAC construction sMGM-MAC.

$\underline{\mathsf{sMGM\text{-}MAC.Gen}()}$

$\rho_t, \rho_h \xleftarrow{\mathcal{U}} Func(n)$
$K \leftarrow (\rho_t, \rho_h)$
**return** $K$

$\underline{\mathsf{sMGM\text{-}MAC.Tag}(K, N, M)}$

$\tau \leftarrow \mathsf{PreTag}(\rho_h, N, M)$
$T \leftarrow \rho_t(\tau)$
**return** $T$

$\underline{\mathsf{PreTag}(\rho_h, N, M)}$

$l \leftarrow |M|_n$
**for** $i = 1 \ldots \ell$ **do**:
  $H_i \leftarrow \rho_h(00 \| \mathrm{str}_{n-2}(N + i - 1))$
$\tau \leftarrow \mathsf{Set11}_r\left(\bigoplus_{i=1}^{l}(M_i \otimes H_i)\right)$
**return** $\tau$

$\underline{\mathsf{sMGM\text{-}MAC.Verify}(K, N, M, T)}$

$\tau \leftarrow \mathsf{PreTag}(\rho_h, N, M)$
$T' \leftarrow \rho_t(\tau)$
**if** $T' \neq T$: **return** false
**return** true

Figure 4: The sMGM-MAC scheme

We claim that there exists an UF-CMA-adversary $\mathcal{D}$, making at most $q_E$ queries to the $Tag$ oracle and at most $q_D$ queries to the $Verify$ oracle, such that

$$\Pr\big[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[\rho_h]}(\mathcal{A}) \to 1\big] \leq \Pr\big[\mathbf{Exp}^{\text{UF-CMA}}_{\mathsf{sMGM\text{-}MAC}}(\mathcal{D}) \to 1\big].$$

Indeed, let us construct the adversary $\mathcal{D}$, that uses the adversary $\mathcal{A}$ as a black box. The adversary $\mathcal{D}$ intercepts the queries of the adversary $\mathcal{A}$ and process them by itself using its own oracles. For encryption/decryption $\mathcal{D}$ implements lazy sampling for $\rho_C$. For tag generation/tag verification the adversary $\mathcal{D}$ implements the padding procedure and sends the appropriate queries to its oracles.

If $\mathcal{A}$ makes a non-trivial valid query $(N, A, C, T)$ to the $Decrypt$ oracle, then the adversary $\mathcal{D}$ decrypts $C$ using $\rho_C$ to obtain a plaintext $P$ and then makes corresponding non-trivial query $(N, M = A\|0^a\|P\|0^c\|len_A\|len_P, T)$ to the $Verify$ oracle. Hence, if the adversary $\mathcal{A}$ forges, then the adversary $\mathcal{D}$ also forges in $\mathbf{Exp}^{\text{UF-CMA}}_{\mathsf{sMGM\text{-}MAC}}$.

Finally, we can apply Corollary 1 from [1] to obtain a bound for $\Pr\big[\mathbf{Exp}^{\text{UF-CMA}}_{\mathsf{sMGM\text{-}MAC}}(\mathcal{D}) \to 1\big]$:

$$\Pr\big[\mathbf{Exp}^{\text{UF-CMA}}_{\mathsf{sMGM\text{-}MAC}}(\mathcal{D}) \to 1\big] \leq \frac{q(q-1)}{2^{n-1}} + \frac{q_D}{2^n}.$$

Summarizing all the obtained bounds, we have

$$\Pr\left[\mathbf{Exp}^{\text{MRAE-int}}_{\mathsf{sMGMs}[E_K]}(\mathcal{A}) \to 1\right] \leq$$
$$\leq \left(\left(\frac{q(q-1)}{2^{n-1}} + \frac{q_D}{2^n}\right) \cdot B_{l+s}^{q_N t_I} + \sum_{i=1}^{q_N \cdot t_I} \mathsf{Adv}^{\text{PRP}}_E(\mathcal{C}_i) \cdot B_{l+s}^{i-1}\right) \cdot B_{q(2l_0+2s+1)} + \mathsf{Adv}^{\text{PRP}}_E(\mathcal{C}_0) \leq$$
$$\leq \left(\frac{q(q-1)}{2^{n-1}} + \frac{q_D}{2^n} + \sum_{i=1}^{q_N \cdot t_I} \mathsf{Adv}^{\text{PRP}}_E(\mathcal{C}_i)\right) \cdot B_{l+s}^{q_N t_I} \cdot B_{q(2l_0+2s+1)} + \mathsf{Adv}^{\text{PRP}}_E(\mathcal{C}_0). \quad (2)$$

Denoting by $\mathcal{C}$ the adversary with the the biggest advantage among $\mathcal{C}_i$, we obtain the statement of the Theorem. □

### 5.3 MRAE security of sMGMs

**Theorem 3.** *For any* MRAE*-adversary* $\mathcal{A}$ *for* sMGMs*, making at most* $q_E$ *queries to the Encrypt oracle and at most* $q_D$ *queries to the Decrypt oracle, where the block-length of associated data in each query is at most* $m_A$*, the block-length of plaintexts and ciphertexts in each query is at most* $m_P$*, the number of distinct nonce values in all queries is at most* $q_N$ *and the number of queries with the same nonce is at most* $q_R$*, there exist* PRP*-adversaries* $\mathcal{B}_0, \mathcal{B}_I$ *and* $\mathcal{B}_C$ *for block cipher* $E$*, such that*

$$\mathsf{Adv}^{\text{MRAE}}_{\mathsf{sMGM}[E,r,l_0,l,1]}(\mathcal{A}) \leq \frac{q^2}{2^{n-1}} + \frac{q^2 \max(l,l_0)}{2^{n-2}} + \frac{q_D}{2^n} + \frac{q^2(2l_0+2s+1)^2}{2^{n+1}} + q_N t_I \frac{(l+s)^2}{2^{n+1}} +$$
$$+ q_N t_C \frac{(q_R l + s)^2}{2^{n+1}} + \mathsf{Adv}^{\text{PRP}}_E(\mathcal{B}_0) + q_N t_I \mathsf{Adv}^{\text{PRP}}_E(\mathcal{B}_I) + q_N t_C \mathsf{Adv}^{\text{PRP}}_E(\mathcal{B}_C),$$

*where* $q = q_E + q_D, s = \lceil k/n \rceil$*,* $t_I = \lceil (m_A + m_P + 2 - l_0)/l \rceil$ *and* $t_C = \lceil (m_P - l_0)/l \rceil$*. Adversary* $\mathcal{B}_0$ *makes at most* $q(2l_0 + 2s + 1)$ *queries to its oracle,* $\mathcal{B}_I$ *makes at most* $l + s$ *queries and* $\mathcal{B}_C$ *makes at most* $q_R l + s$ *queries.*

*Proof.* We start with replacing all block ciphers with random functions. This will allow us to use the MRAE security theorem for SIV constructions from [14] to bound the security of sMGMs by PRF security of sMGM-MAC and IND-CPA$ security of CTR-KM (with random IV and independent random functions used for processing each section).

First of all, we replace $E_K$ with a random function $\rho_0$. As in the previous proof, we firstly replace it with a random permutation, building a PRP adversary $\mathcal{B}_0$. After that we use PRP/PRF Switching Lemma to replace random permutation with a random function. It is easy to see, that there are at most $q(2l_0 + 2s + 1)$ calls to $E_K$, hence, we have

$$\Pr\left[\mathbf{Exp}^{\text{MRAE}-0}_{\mathsf{sMGMs}[E_K,E]}(\mathcal{A}) \to 1\right] \leq \Pr\left[\mathbf{Exp}^{\text{MRAE}-0}_{\mathsf{sMGMs}[\rho_0,E]}(\mathcal{A}) \to 1\right] +$$
$$+ \frac{q(2l_0+2s+1)(q(2l_0+2s+1)-1)}{2^{n+1}} + \mathsf{Adv}^{\text{PRP}}_E(\mathcal{B}_0).$$

At the next step we replace all other block ciphers with random functions as in the previous proof. However, we can't use Bernstein's lemma to switch from pseudorandom permutation to pseudorandom function, thus we have to apply PRP/PRF Switching Lemma [10]. There are at most $q_N \cdot t_I$ keys in the tag generation part and $q_N \cdot t_C$ keys in the encryption part. We construct adversaries $\mathcal{B}_i^I$ and $\mathcal{B}_i^C$ for each block cipher used in the tag generation and encryption parts respectively. For each block cipher in the tag generation part an adversary $\mathcal{B}_i^I$ makes at most $l + s$ queries (for processing the section

and re-keying). For each block cipher in the encryption part an adversary $\mathcal{B}_i^C$ makes at most $q_R l + s$ queries (we multiply by $q_R$ since block cipher inputs for $\Gamma_j$ generation are distinct even if the same nonce is used). We denote a mode with independent random functions by $\mathsf{sMGMs}[\rho_0, \hat{\rho}]$. At this point we have

$$\Pr\Big[\mathbf{Exp}^{\text{MRAE}-0}_{\mathsf{sMGMs}[\rho_0,E]}(\mathcal{A}) \to 1\Big] \le \Pr\Big[\mathbf{Exp}^{\text{MRAE}-0}_{\mathsf{sMGMs}[\rho_0,\hat{\rho}]}(\mathcal{A}) \to 1\Big] + q_N t_I \frac{(l+s)(l+s-1)}{2^{n+1}} + \\ + q_N t_C \frac{(q_R l + s)(q_R l + s - 1)}{2^{n+1}} + \sum_{i=1}^{q_N \cdot t_I} \mathsf{Adv}^{\text{PRP}}_E(\mathcal{B}_i^I) + \sum_{i=1}^{q_N \cdot t_C} \mathsf{Adv}^{\text{PRP}}_E(\mathcal{B}_i^C).$$

In sequel we denote by $\mathcal{B}_I$ ($\mathcal{B}_C$) an adversary with the biggest advantage among $\mathcal{B}_i^I$ ($\mathcal{B}_i^C$ resp.).

We will denote by $\mathsf{CTR\text{-}KM}[\hat{\rho_C}]$ a CTR-KM (see Figure 2) construction, in which for each unique nonce in each re-keying section an independent random function is used to produce $\Gamma_i$ (in queries with a repeating nonce the same sequence of independent functions is used). Encryption and decryption algorithms for $\mathsf{CTR\text{-}KM}[\hat{\rho_C}]$ are defined naturally.

Since inputs to random functions in the tag generation and encryption parts of sMGMs do not intersect, due to Statement 1, we claim, that these two parts are independent from each other. Finally we apply Theorem 1 [14]. There exist adversaries $\mathcal{D}$ and $\mathcal{C}$ such that

$$\Pr\Big[\mathbf{Exp}^{\text{MRAE}-0}_{\mathsf{sMGMs}[\rho_0,\hat{\rho}]}(\mathcal{A}) \to 1\Big] - \Pr\Big[\mathbf{Exp}^{\text{MRAE}-1}_{\mathsf{sMGMs}[E_{\mathcal{K}},E]}(\mathcal{A}) \to 1\Big] = \\ = \Pr\Big[\mathbf{Exp}^{\text{MRAE}-0}_{\mathsf{sMGMs}[\rho_0,\hat{\rho}]}(\mathcal{A}) \to 1\Big] - \Pr\Big[\mathbf{Exp}^{\text{MRAE}-1}_{\mathsf{sMGMs}[\rho_0,\hat{\rho}]}(\mathcal{A}) \to 1\Big] = \\ = \mathsf{Adv}^{\text{MRAE}}_{\mathsf{sMGMs}[\rho_0,\hat{\rho}]}(\mathcal{A}) \le \mathsf{Adv}^{\text{PRF}}_{\mathsf{sMGM\text{-}MAC}[\rho_t,\rho_h]}(\mathcal{D}) + \mathsf{Adv}^{\text{IND-CPA\$}}_{\mathsf{CTR\text{-}KM}[\hat{\rho}_C]}(\mathcal{C}) + \frac{q_D}{2^n}.$$

The only thing left is to derive a bound for $\mathsf{Adv}^{\text{IND-CPA\$}}_{\mathsf{CTR\text{-}KM}[\hat{\rho}_C]}(\mathcal{C})$. The idea is similar to the classical proof of IND-CPA\$ security of CTR from [6]. In that proof the bad case happens if counters in two queries overlap. In our case, since each section is processed with its own independent random function, the bad case happens if for two queries counters in the same section overlap. We denote that event by Bad and an event, that counters overlap in queries $j_1$ and $j_2$, by $\mathsf{Bad}_{j_1 j_2}$.

We notice, that if in queries $j_1$ and $j_2$ counters overlap in the $i$-th section, then the following inequality holds

$$IV_{j_1} + k'(i) - l'(i) + 1 \le IV_{j_2} + k'(i) \le IV_{j_1} + k'(i) + l'(i) - 1 \Leftrightarrow$$

$$IV_{j_1} - l'(i) + 1 \le IV_{j_2} \le IV_{j_1} + l'(i) - 1,$$

where $l'(i)$ is a length of the $i$-th section (equal to $l_0$ if $i = 0$ and to $l$ otherwise) and $k'(i)$ is the counter offset in the begining of the $i$-th section (equal to 0 if $i = 0$ and to $l_0 + l(i-1)$ otherwise). Hence, for the probability of the event $\mathsf{Bad}_{j_1 j_2}$ we have

$$\Pr[\mathsf{Bad}_{j_1 j_2}] \;=\; \Pr\Big[IV_{j_1}, IV_{j_2} \xleftarrow{\mathcal{U}} \{0,1\}^{n-2} :\; \exists i :\; IV_{j_1} - l'(i) + 1 \le IV_{j_2} \le IV_{j_1} + l'(i) - 1\Big].$$

Since for every $0 \le i \le t_C$ it is true, that $l'(i) \le \max(l_0, l)$, we can bound the

probability in the following way

$$\Pr\Big[IV_{j_1}, IV_{j_2} \xleftarrow{\mathcal{U}} \{0,1\}^{n-2} :\ \exists i :\ IV_{j_1} - l'(i) + 1 \le IV_{j_2} \le IV_{j_1} + l'(i) - 1\Big] \le$$
$$\le \Pr\Big[IV_{j_1}, IV_{j_2} \xleftarrow{\mathcal{U}} \{0,1\}^{n-2} : IV_{j_1} - \max(l_0, l) + 1 \le IV_{j_2} \le IV_{j_1} + \max(l_0, l) - 1\Big] =$$
$$= \frac{2\max(l_0, l) - 1}{2^{n-2}}.$$

From that we obtain a bound for the event $\Pr[\mathsf{Bad}]$ (and, therefore for the adversarial advantage), going through all possible pairs of queries:

$$\mathsf{Adv}^{\text{IND-CPA\$}}_{\mathsf{CTR\text{-}KM}[\rho]}(\mathcal{C}) \le \Pr[\mathsf{Bad}] \le \sum_{1 \le j_1 < j_2 \le q} \Pr[\mathsf{Bad}_{j_1 j_2}] \le$$
$$\le \frac{q(q-1)}{2} \cdot \frac{2\max(l_0, l) - 1}{2^{n-2}} \le \frac{q^2 \max(l_0, l)}{2^{n-2}}.$$

Finally, using Lemma 1 from [1] to obtain a bound for $\mathsf{Adv}^{\text{PRF}}_{\mathsf{sMGM\text{-}MAC}[\rho_t, \rho_h]}(\mathcal{D})$ and connecting everything together, we have the required bound. □

## 6 Open problems

In the future work we are going to develop the proposed parameterizable AEAD conception by adding new security features provided by the mode with respect to exploitation properties. Such properties as leakage resilience, RUP-security, Key-dependent messages security are to be considered in particular. We believe that the designated goal can be achieved in sMGM without significant difficulties by combining the building blocks of the mode in an appropriate way.

## References


[1] Liliya Akhmetzyanova, Evgeny Alekseev, Alexandra Babueva, Andrey Bozhko, Stanislav Smyshlyaev, (2022) *Misuse-resistant MGM2 mode*, International Journal of Open Information Technologies, Vol 10, No 1.

[2] Akhmetzyanova L., Alekseev E., Smyshlyaev S., Oshkin I. (2020) *On Internal Re-keying.* In: van der Merwe T., Mitchell C., Mehrnezhad M. (eds) Security Standardisation Research. SSR 2020. Lecture Notes in Computer Science, vol 12529. Springer, Cham. https://doi.org/10.1007/978-3-030-64357-7_2

[3] Andreeva E., Bogdanov A., Luykx A., Mennink B., Mouha N., Yasuda K. (2014) *How to Securely Release Unverified Plaintext in Authenticated Encryption.* In: Sarkar P., Iwata T. (eds) Advances in Cryptology – ASIACRYPT 2014. ASIACRYPT 2014. Lecture Notes in Computer Science, vol 8873. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-45611-8_6

[4] Davide Bellizia and Olivier Bronchain and Gaëtan Cassiers and Vincent Grosso and Chun Guo and Charles Momin and Olivier Pereira and Thomas Peters and François-Xavier Standaert, *Mode-Level vs. Implementation-Level Physical Security in Symmetric Cryptography: A Practical Guide Through the Leakage-Resistance Jungle*, Cryptology ePrint Archive, Report 2020/211, 2020, https://eprint.iacr.org/2020/211

[5] Brandstetter L., Fischlin M., Schröder R.L., Yonli M. (2020) *On the Memory Fault Resilience of TLS 1.3.* In: van der Merwe T., Mitchell C., Mehrnezhad M. (eds) Security Standardisation Research. SSR 2020. Lecture Notes in Computer Science, vol 12529. Springer, Cham. https://doi.org/10.1007/978-3-030-64357-7_1

[6] Bellare M., Rogaway P. *Introduction to modern cryptography* //Ucsd Cse. – 2005. – T. 207. – C. 207.

[7] Bernstein, D.J.: *Stronger Security Bounds for Permutations* (2005), http://cr.yp.to/papers.html (accessed on May 31, 2012)

[8] John Black, Phillip Rogaway, and Thomas Shrimpton. 2002. *Encryption-Scheme Security in the Presence of Key-Dependent Messages*. In Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography (SAC '02). Springer-Verlag, Berlin, Heidelberg, 62–75.

[9] Chakraborty, D., López, C.M. & Sarkar, P. *Disk encryption: do we need to preserve length?*. J Cryptogr Eng 8, 49–69 (2018). https://doi.org/10.1007/s13389-016-0147-0

[10] D. Chang and M. Nandi, *A Short Proof of the PRP/PRF Switching Lemma* // IACR ePrint Archive, 2008, Report 2008/078, https://eprint.iacr.org/2008/078.

[11] Federal Agency on Technical Regulating and Metrology, *Information technology. Cryptographic data security. Authenticated encryption block cipher operation modes*, R 1323565.1.026-2019, 2019.

[12] Gueron S., Lindell Y. *GCM-SIV: full nonce misuse-resistant authenticated encryption at under one cycle per byte* //Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. – 2015. – C. 109-119.

[13] Hoang V.T., Krovetz T., Rogaway P. (2015) *Robust Authenticated-Encryption AEZ and the Problem That It Solves*. In: Oswald E., Fischlin M. (eds) Advances in Cryptology – EUROCRYPT 2015. EUROCRYPT 2015. Lecture Notes in Computer Science, vol 9056. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-46800-5_2

[14] Rogaway P., Shrimpton T. *A provable-security treatment of the key-wrap problem* //Annual International Conference on the Theory and Applications of Cryptographic Techniques. – Springer, Berlin, Heidelberg, 2006. – C. 373-390.

[15] Smyshlyaev, S., Nozdrunov, V., Shishkin, V., and E. Smyshlyaeva *Multilinear Galois Mode (MGM)* // 2019, <https://tools.ietf.org/html/draft-smyshlyaev-mgm-17>

# A Security models

This section introduces models for an adversary that may repeat nonces in its queries. We begin with the strongest model, which formalizes both integrity and confidentiality properties – MRAE («Misuse-Resistant Authenticated Encryption - integrity»), firstly introduced in [14].

**Definition 1.** *For an AEAD-scheme* $\Pi$ *the advantage of a* MRAE*-adversary* $\mathcal{A}$ *is defined as follows:*

$$\mathsf{Adv}^{\text{MRAE}}_{\Pi}(\mathcal{A}) = \Pr\big[\mathbf{Exp}^{\text{MRAE}-1}_{\Pi}(\mathcal{A}) \to 1\big] - \Pr\big[\mathbf{Exp}^{\text{MRAE}-0}_{\Pi}(\mathcal{A}) \to 1\big],$$

*where experiments* $\mathbf{Exp}^{\text{MRAE-int}}_{\Pi}$ *are defined below:*

| $\mathbf{Exp}^{\text{MRAE}-b}_{\Pi}(\mathcal{A})$ | *Oracle* $Encrypt^b(N, A, P)$ | *Oracle* $Decrypt^b(N, A, C, T)$ |
|---|---|---|
| $K \xleftarrow{\$} \Pi.\mathsf{Gen}(\,)$ | **if** $(N, A, P, \cdot, \cdot) \in sent$ : | **if** $(N, A, \cdot, C, T) \in sent$ : |
| $sent \leftarrow \emptyset$ | **return** $\perp$ | **return** $\perp$ |
| $b' \xleftarrow{\$} \mathcal{A}^{Encrypt^b, Decrypt^b}(\,)$ | **if** $b = 1$ : | **if** $b = 1$ : |
| **return** $b'$ | $(C, T) \leftarrow \Pi.\mathsf{Enc}(K, N, A, P)$ | **return** $\Pi.\mathsf{Dec}(K, N, A, C, T)$ |
| | **else** : | **else** : |
| | $C \parallel T \xleftarrow{\mathcal{U}} \{0,1\}^{\lvert P\rvert + s}$ | **return** $\perp$ |
| | $sent \leftarrow sent \cup \{(N, A, P, C, T)\}$ | |
| | **return** $(C, T)$ | |

We also separately define a model formalizing the integrity property of AEAD schemes in nonce misuse setting – MRAE-int.

**Definition 2** (MRAE-int)**.** *For an AEAD-scheme* $\Pi$ *the advantage of a* MRAE-int*-adversary* $\mathcal{A}$ *is defined as follows:*

$$\mathsf{Adv}^{\text{MRAE-int}}_{\Pi}(\mathcal{A}) = \Pr\big[\mathbf{Exp}^{\text{MRAE-int}}_{\Pi}(\mathcal{A}) \to 1\big],$$

*where experiment* $\mathbf{Exp}^{\text{MRAE-int}}_{\Pi}$ *is defined below:*

$\mathbf{Exp}_{\Pi}^{\text{MRAE-int}}(\mathcal{A})$

$K \xleftarrow{\$} \Pi.\mathsf{Gen}(\ )$
$sent \leftarrow \emptyset$
$win \leftarrow \mathsf{false}$
$\mathcal{A}^{Encrypt, Decrypt}(\ )$
**return** $win$

*Oracle* $Encrypt(N, A, P)$

$(C, T) \leftarrow \Pi.\mathsf{Enc}(K, N, A, P)$
$sent \leftarrow sent \cup \{(N, A, C, T)\}$
**return** $(C, T)$

*Oracle* $Decrypt(N, A, C, T)$

$P \leftarrow \Pi.\mathsf{Dec}(K, N, A, C, T)$
**if** $(P \neq \perp) \wedge ((N, A, C, T) \notin sent)$:
  $win \leftarrow \mathsf{true}$
**return** $P$

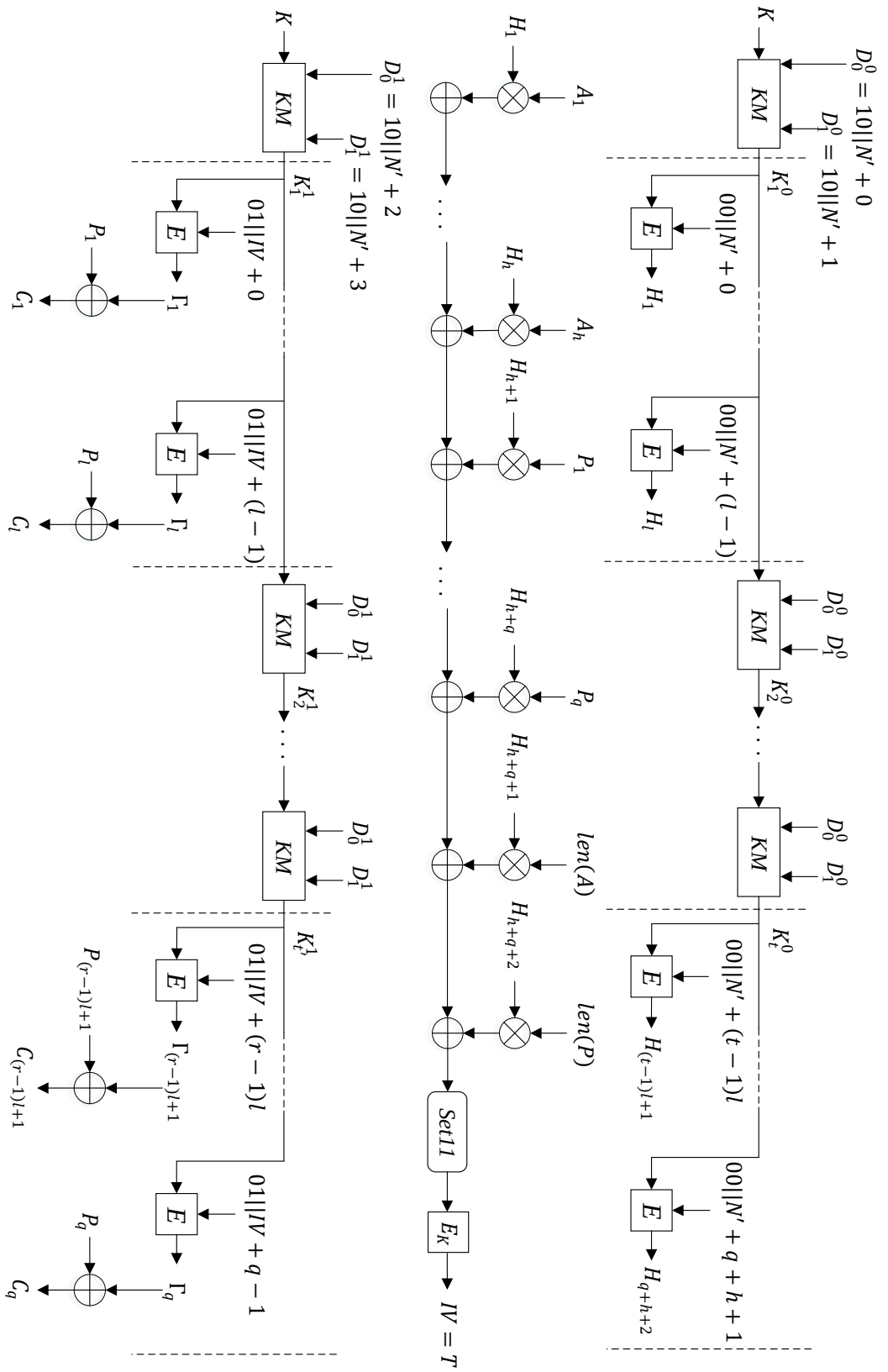


Figure 5: sMGM mode with $l_0 = 0, s = 2$ (sketch)