Security of Multilinear Galois Mode (MGM)

Liliya Akhmetzyanova, Evgeny Alekseev,
Grigory Karpunin, Vladislav Nozdrunov

Crypto-Pro LLC, Moscow, Russia
{lah,alekseev,karpunin}@cryptopro.ru
Technical Committee for Standardization «Cryprography and Security Mechanisms» (TC 26)
nozdrunov_vi@tc26.ru

Abstract

In this paper we analyze the new AEAD mode called the Multilinear Galois Mode (MGM) originally proposed in CTCrypt 2017. This mode is currently considered in the Russian Standardization system as the main contender to be adopted as a standard AEAD mode. The analysis of the MGM mode was carried out in the paradigm of provable security, in other words, lower security bounds were obtained for the Privacy and Authenticity notions. These bounds show that the privacy and authenticity of this mode is provably guaranteed (under security of the used block cipher) up to the birthday paradox bound.

Keywords: AEAD mode, privacy, integrity, provable security

1 Introduction

Authenticated encryption with associated data schemes (AEAD), which aim at providing both privacy and integrity (authenticity) of data, have gained renewed attention in the light of the recently adopted TLS 1.3 [12] which requires the mandatory usage of such schemes.

The main advantages of the AEAD schemes are their exploitation transparency and simplicity. Indeed, explicitly defined construction and unified interface facilitate correct implementing and transparent embedding into high-level schemes. Moreover, the usage of one key for providing both privacy and authenticity eliminates the need for additional key diversification usually used for producing a couple of independent keys for «generic compositions», meaning making black-box use of a given symmetric encryption scheme and a given MAC. This feature allows to claim (in addition to obvious performance improvement) that the AEAD schemes provide more guaranteed security compared to the generic compositions since their security is held under fewer assumptions.

In this paper we analyze the new AEAD mode called the Multilinear Galois Mode (MGM) originally proposed in [10] and later described in [9]. This mode is currently considered in the Russian Standardization system as the main contender to be adopted as a standard AEAD mode. The structure of the mode is as follows. The MGM plaintext encryption procedure is quite similar to encryption in the counter mode (certainly, in the CTR2 mode [13]). The main element of the MGM authentication procedure is a multilinear function with secret coefficients produced in the same way as the secret masking blocks used for plaintext encryption. This construction allows to keep such advantages of the CTR2 mode as parallelization, online, inverse-free and availability of precomputations.

The analysis of the MGM mode was carried out in the paradigm of provable security, in other words, lower security bounds were obtained for security notions relevant for AEAD modes (the Privacy and Authenticity notions).

This paper is structured as follows. Firstly, in Section 2 we introduce preliminaries. In Section 3 and Section 4 we describe encryption and decryption procedures of the MGM mode and talk about their design rationales. In Section 5 we remind accompanying security notions and introduce auxiliary security notions. In Section 6 we provide two theorems about privacy and authenticity of the MGM mode.

2 Preliminaries

By $\{0,1\}^u$ we denote the set of u-component bit strings and by $\{0,1\}^*$ we denote the set of all bit strings of finite length. Let 0^u be the string, consisting of u zeros. For bit strings U and V we denote by $U\|V$ their concatenation. Let $|U|$ be the bit length of the string U. We denote by $|U|_u = \lceil |U|/u \rceil$ the length of the string U in u-bit blocks.

Denote by $\{0,1\}^{n\times m}$ the set of all m-tuples where elements of an m-tuple are n-bit blocks, m is called a length of tuple. By $\{0,1\}^{n\times *}$ we denote the set of all tuples of finite length. For m-tuple X we denote by $\{X\}$ the set of all elements of X. To reduce expressions in formulas, for $x \in \{0,1\}^n$, $X, Y \in \{0,1\}^{n\times *}$, we use the natural notations $x \in X$, $x \notin X$, and $X \cap Y$ instead of $x \in \{X\}$, $x \notin \{X\}$, and $\{X\} \cap \{Y\}$.

For a bit string U and a positive integer $l \leqslant |U|$ let $\mathrm{msb}_l(U)$ ($\mathrm{lsb}_l(U)$) be the string, consisting of the leftmost (rightmost) l bits of U. For integers $l > 0$ and $i \geqslant 0$ let $\mathrm{str}_l(i)$ be l-bit representation of i with the least significant bit on the right. For an integer $l > 0$ and a bit string $U \in \{0,1\}^l$ let $\mathrm{int}(U)$ be an integer i such that $\mathrm{str}_l(i) = U$.

Let $inc_r(U)$ be the function, which takes the input $L\|R$, where $L, R \in \{0,1\}^{n/2}$, and outputs the string $L\|\mathrm{str}_{n/2}(\mathrm{int}(R) + 1 \bmod 2^{n/2})$. Let $inc_l(U)$ be the function, which takes the input $L\|R$, where $L, R \in \{0,1\}^{n/2}$, and outputs the string $\mathrm{str}_{n/2}(\mathrm{int}(L) + 1 \bmod 2^{n/2})\|R$.

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 (or just a *cipher*) with block size n and key size k is a permutation family $\big(E_K \in Perm(\{0,1\}^n) \mid K \in \{0,1\}^k\big)$, where K is a key. If the value s is chosen from a set S uniformly at random, then we denote $s \overset{\mathcal{U}}{\leftarrow} S$.

Hereinafter we denote random variables using tilde (e.g. $\widetilde{\lambda}$) and its specific values without tilde (i.e. λ). Let $\widetilde{\Lambda} = (\widetilde{\lambda}_1, \ldots, \widetilde{\lambda}_m)$ be an m-tuple of random variables $\widetilde{\lambda}_i \colon \Omega \to \{0,1\}^n$, $i = 1, \ldots, n$, where Ω is a finite probability space. Let Λ be a possible value of m-tuple $\widetilde{\Lambda}$. By $\widetilde{\Lambda} \setminus \{\widetilde{\lambda}_{i_1}, \ldots, \widetilde{\lambda}_{i_s}\}$ we denote the tuple $\widetilde{\Lambda}$ from which the random variables $\widetilde{\lambda}_{i_1}, \ldots, \widetilde{\lambda}_{i_s}$ are ejected. And by $\Lambda \setminus \{\widetilde{\lambda}_{i_1}, \ldots, \widetilde{\lambda}_{i_s}\}$ denote a possible value of $\widetilde{\Lambda} \setminus \{\widetilde{\lambda}_{i_1}, \ldots, \widetilde{\lambda}_{i_s}\}$. For $\omega \in \Omega$, let $\widetilde{\Lambda}(\omega)$ denote the m-tuple $(\widetilde{\lambda}_1(\omega), \ldots, \widetilde{\lambda}_1(\omega))$.

By $\Lambda\, coll$ we denote a predicate to be equal to $true$, if there exist coincide elements in Λ, and $false$, otherwise. Denote by $\Lambda\, \overline{coll}$ the negation of the predicate $\Lambda\, coll$. For tuple $\widetilde{\Lambda}$, denote by $\widetilde{\Lambda}\, coll$ an event $\{\omega \in \Omega \mid \widetilde{\Lambda}\, coll = true\}$, i.e. the tuple of output values Λ doesn't contain coincide elements. By $\widetilde{\Lambda}\, \overline{coll}$ denote the negation of the event $\widetilde{\Lambda}\, coll$.

Finally, by $\widetilde{\lambda} \in_{val} \widetilde{\Lambda}$ denote the event $\{\omega \in \Omega \mid \widetilde{\lambda}(\omega) \in \widetilde{\Lambda}(\omega)\}$.

3 MGM Description

An additional parameter that defines the functioning of the MGM mode is the size s of the authentication tag (in bits). The value of s must be fixed for a particular protocol, $32 \leq s \leq 128$.

3.1 MGM Encryption

The MGM encryption algorithm based on a cipher E takes as inputs a key $K \in \{0,1\}^k$, a nonce $N \in \{0,1\}^{n-1}$, a plaintext $P \in \{0,1\}^*$, $0 \leqslant |P| < 2^{n/2}$, and associated data $A \in \{0,1\}^*$, $0 \leqslant |A| \leq 2^{n/2}$. The length of the associated data A and of the plaintext P must be such that $0 < |A| + |P| \leqslant n \cdot 2^{n/2}$. The outputs of this algorithm are a ciphertext $C \in \{0,1\}^{|P|}$ and a tag $T \in \{0,1\}^s$ that are calculated as follows:

1. The plaintext P and associated data A are divided into sequences of n-bit blocks (perhaps except last one):

$$A = A_1\| \ldots \|A_{h-1}\|A_h^*,\ A_j \in \{0,1\}^n, A_h^* \in \{0,1\}^a,$$
$$P = P_1\| \ldots \|P_{t-1}\|P_t^*,\ P_i \in \{0,1\}^n, P_t^* \in \{0,1\}^c,$$

   where $j = 1, 2, \ldots, h-1$; $i = 1, 2, \ldots, t-1$; $1 \leqslant a, c \leqslant n$ and $h + t > 0$.

2. Encryption:

$$\begin{cases} Y_1 \;=\; E_K(0\|N), & \\ Y_i = inc_r(Y_{i-1}), & 2 \leqslant i \leqslant t, \\ C_i = P_i \oplus E_K(Y_i), & 1 \leqslant i \leqslant t-1, \\ C_t^* = P_t^* \oplus \mathrm{msb}_c(E_K(Y_t)). & \end{cases}$$

3. Blocks $A_h^* \in \{0,1\}^a$ and $C_t^* \in \{0,1\}^c$ are padded if needed:

$$\begin{cases} A_h = A_h^* \| 0^{n-a}, \\ C_t = C_t^* \| 0^{n-c}. \end{cases}$$

4. Authentication tag calculation:

$$T = \mathrm{msb}_s\left(E_K\left(\sum_{i=1}^{h} H_i \cdot A_i \oplus \sum_{j=1}^{t} H_{h+j} \cdot C_j \oplus H_{h+t+1} \cdot \left(\mathrm{str}_{n/2}(|A|)\|\mathrm{str}_{n/2}(|C|)\right)\right)\right),$$

where $H_i = E_K(Z_i)$, $\cdot$ and $\oplus$ ($\sum$) is multiplication and summation in $GF(2^n)$ (here bit-string are interpreted as field elements in the standard way) and values Z_i, $i = 1, 2, \ldots$ are defined as follows:

$$\begin{cases} Z_1 = E_K(1\|N), \\ Z_i = inc_l(Z_{i-1}),\; 2 \leqslant i \leqslant h+t+1. \end{cases}$$

The encryption process is illustrated in Fig. 1.

3.2 MGM Decryption

The MGM decryption algorithm based on a cipher E takes as inputs a key $K \in \{0,1\}^k$, a nonce $N \in \{0,1\}^{n-1}$, a ciphertext $C \in \{0,1\}^*$, $0 \leqslant |C| < 2^{n/2}$, and associated data $A \in \{0,1\}^*$, $0 \leqslant |A| < 2^{n/2}$. The length of the associated data A and of the ciphertext C must be such that $0 < |A| + |C| \leqslant n \cdot 2^{n/2}$. The algorithm outputs a plaintext $P \in \{0,1\}^{|C|}$ or Error that are calculated as follows:

1. Ciphertext C and associated data A are divided into sequences of n-bit blocks (perhaps, except the last one):

$$A = A_1\| \ldots \|A_{h-1}\|A_h^*,\; A_j \in \{0,1\}^n, A_h^* \in \{0,1\}^a,$$
$$C = C_1\| \ldots \|C_{t-1}\|C_t^*,\; C_i \in \{0,1\}^n, C_t^* \in \{0,1\}^c,$$

where $j = 1, 2, \ldots, h-1$, $i = 1, 2, \ldots, t-1$, $1 \leqslant a, c \leqslant n$ and $h + t > 0$.

2. Blocks $A_h^* \in \{0,1\}^a$ and $C_t^* \in \{0,1\}^c$ are padded if needed:

$$\begin{cases} A_h = A_h^* \| 0^{n-a}, \\ C_t = C_t^* \| 0^{n-c}. \end{cases}$$

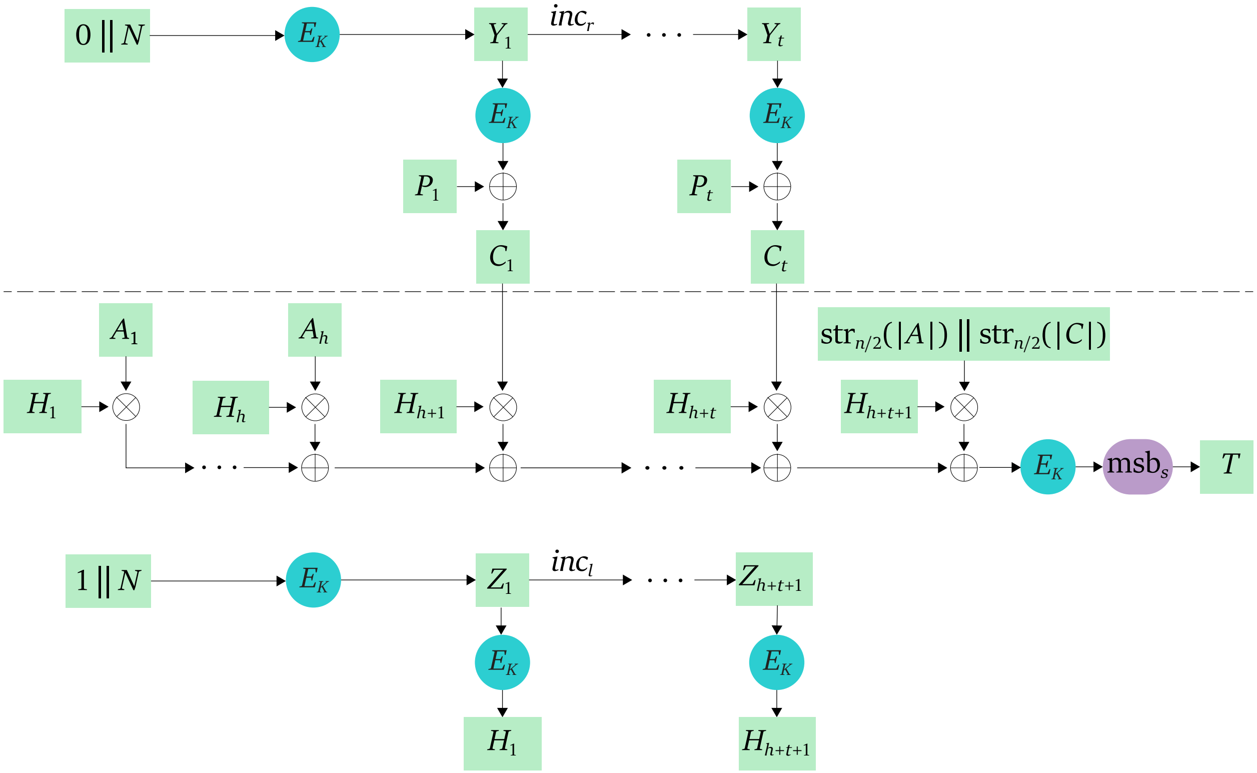

Figure 1: MGM Encryption Procedure for full block messages.

3. Authentication tag calculation:

$$\hat{T} = \mathrm{msb}_s\left(E_K\left(\sum_{i=1}^{h} H_i \cdot A_i \oplus \sum_{j=1}^{t} H_{h+j} \cdot C_j \oplus H_{h+t+1} \cdot \left(\mathrm{str}_{n/2}(|A|)\|\mathrm{str}_{n/2}(|C|)\right)\right)\right),$$

   where $H_i = E_K(Z_i)$, $\cdot$ and $\oplus$ $(\sum)$ is multiplication and summation in $GF(2^n)$, where n is the block size of the used block cipher, and values Z_i, $i = 1, 2, \ldots$ are defined as follows:

$$\begin{cases} Z_1 = E_K(1\|N), \\ Z_i = inc_l(Z_{i-1}),\ 2 \leqslant i \leqslant h+t+1. \end{cases}$$

4. Authentication tag verification:
   Verify the equality $\hat{T} = T$. If $\hat{T} \neq T$, then output Error, else go to step 5.
5. Decryption:

$$\begin{cases} Y_1 \ = \ E_K(0\|N), & \\ Y_i = inc_r(Y_{i-1}), & 2 \leqslant i \leqslant t, \\ P_i = C_i \oplus E_K(Y_i), & 1 \leqslant i \leqslant t-1, \\ P_t^* = C_t^* \oplus \mathrm{msb}_c(E_K(Y_t)). & \end{cases}$$

4 Rationale

From the operational point of view the MGM mode is designed to be parallelizeable, inverse free, online and to provide availability of precomputations.

Parallelizability of the MGM mode is achieved due to its counter-type structure and the usage of the multilinear function for authentication. Indeed, both encryption blocks $E_K(Y_i)$ and authentication blocks H_i are produced in the counter mode manner, and the multilinear function determined by H_i is parallelizeable in itself. Additionally, the counter-type structure of the mode provides the inverse free property.

The online property means the possibility to process message even if it is not completely received (so its length is unknown). To provide this property the MGM mode uses blocks $E_K(Y_i)$ and H_i which are produced basing on two independent source blocks Y_i and Z_i.

Availability of precomputations for the MGM mode means the possibility to calculate H_i and $E_K(Y_i)$ even before data is retrieved. It is holds due to again the usage of counters for calculating them.

The MGM mode incorporates some mechanisms for advancing cryptographic properties. Further we note the main ones:

- *Different procedures generating the counter values Y_i and Z_i.* The procedures inc_r and inc_l are chosen to minimize intersection (if it happens) between the sets of counter values $\{Y_i\}$ and $\{Z_i\}$.
- *Multilinear function for authentication.* It allows to resist the small subgroup attacks [7].
- *Ciphering of the multilinear function output.* This procedure allows to resist Ferguson's attack [4].
- *Ciphering of the nonces $(0||N)$ and $(1||N)$.* The aim of this ciphering is to minimize the number of plaintext/ciphertext pairs of blocks known to an adversary. Small number of these pairs allows to resist attacks that need substantial amount of such material (e.g., linear [8] and differential [2] cryptanalysis, side-channel attacks [11]).

5 Security Notions

We model an adversary using an interactive probabilistic algorithm that has access to one or more oracles. In the case when we need to bring to attention that the adversary $\mathcal{A}$ has access to some oracle $\mathcal{O}$ we use the notation $A^{\mathcal{O}}$. Denote by $\mathcal{A} \Rightarrow val$ the event when an algorithm $\mathcal{A}$ returns a value val as a result of its work. Denote by $\mathbf{Adv}_{\mathrm{S}}^{\mathrm{M}}(\mathcal{A})$ the measure of the success of the adversary $\mathcal{A}$ in realizing a certain threat, defined by the security notion M, for the cryptographic scheme S. The formal definition of this measure will be given in each specific case.

Block cipher. Standard security notions for block ciphers are PRP-CPA («Pseudo Random Permutation under Chosen Plaintext Attack») and PRF («Pseudo Random Function») (see, e.g., [1]).

For the PRP-CPA notion an adversary $\mathcal{A}$ has access to an oracle E_K, where K is chosen at random, or a random permutation oracle π. The adversary makes queries $P \in \{0,1\}^n$. The oracle E_K returns $E_K(P)$ and the permutation oracle π returns $\pi(P)$. At the end of its work the adversary returns 1 or 0.

For an adversary $\mathcal{A}$ and a cipher E with parameters n and k define

$$\mathbf{Adv}_{E}^{\text{PRP-CPA}}(\mathcal{A}) = \Pr\left[K \overset{\mathcal{U}}{\leftarrow} \{0,1\}^k : \mathcal{A}^{E_K} \Rightarrow 1\right] - \Pr\left[\pi \overset{\mathcal{U}}{\leftarrow} Perm(\{0,1\}^n) : \mathcal{A}^{\pi} \Rightarrow 1\right],$$

where the probabilities are defined over the randomness of $\mathcal{A}$ and the choices of K and π.

The PRF notion is defined in the same way as PRP-CPA except for the random permutation $\pi \overset{\mathcal{U}}{\leftarrow} Perm(\{0,1\}^n)$, which is replaced by the random function $\rho \overset{\mathcal{U}}{\leftarrow} Func(\{0,1\}^n)$:

$$\mathbf{Adv}_{E}^{\text{PRF}}(\mathcal{A}) = \Pr\left[K \overset{\mathcal{U}}{\leftarrow} \{0,1\}^k : \mathcal{A}^{E_K} \Rightarrow 1\right] - \Pr\left[\rho \overset{\mathcal{U}}{\leftarrow} Func(\{0,1\}^n) : \mathcal{A}^{\rho} \Rightarrow 1\right].$$

AEAD mode. Standard security notions for the AEAD modes are Privacy and Authenticity (see, e.g., [14]). Consider them for the abstract AEAD_E mode, where E is the underlined cipher with parameters n and k. For simplicity, below we consider the case where a ciphertext has the same length as a plaintext and an authentication tag of size s can be treated separately from ciphertext.

In the current paper a block cipher E is assumed to be a family of *all* permutations $Perm(\{0,1\}^n)$. This assumption is standard for the cryptographic analysis of block cipher modes of operation (see, e.g., [5]).

Privacy. An adversary $\mathcal{A}$ has access to an encryption oracle $\mathcal{E}$ or a random-bits oracle \$. Before starting the work the encryption oracle chooses a permutation $\pi \overset{\mathcal{U}}{\leftarrow} Perm(\{0,1\}^n)$. The adversary makes queries (N, A, P), where N is a nonce, A is an associated data and P is a plaintext. The random-bits oracle returns (C, T), where $C \| T \overset{\mathcal{U}}{\leftarrow} \{0,1\}^{|P|+s}$. The encryption oracle returns (C, T), $C \in \{0,1\}^{|P|}$, $T \in \{0,1\}^s$, — the result of $\text{AEAD}_{Perm(\{0,1\}^n)}$ encryption of (N, A, P) for permutation π. At the end of its work the adversary returns 1 or 0.

For the $\text{AEAD}_{Perm(\{0,1\}^n)}$ mode define

$$\mathbf{Adv}_{\text{AEAD}_{Perm(\{0,1\}^n)}}^{\text{Priv}}(\mathcal{A}) = \Pr\left[\pi \overset{\mathcal{U}}{\leftarrow} Perm(\{0,1\}^n) : \mathcal{A}^{\mathcal{E}} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{\$} \Rightarrow 1\right],$$

where the probabilities are defined over the randomness of $\mathcal{A}$, the choices of π and randomness of the random-bits oracle, respectively. We consider a set of nonce-respecting adversaries, which choose N unique for each query.

Authenticity. An adversary $\mathcal{A}$ has access to an encryption oracle $\mathcal{E}$. Before starting the work the oracle chooses a permutation $\pi \overset{\mathcal{U}}{\leftarrow} Perm(\{0,1\}^n)$. The adversary interacts with the encryption oracle $\mathcal{E}$ in the same way as described in the Privacy notion. At the end of its work the adversary outputs (N, A, C, T), where N is a nonce, A is an associated data, C is a ciphertext and T is an authentication tag. The adversary forges if (N, A, C, T) is a valid message and the value (C, T) was not returned by the encryption oracle as a response to the query (N, A, P) for some P. As in the Privacy notion, we assume that $\mathcal{A}$ is nonce-respecting to encryption oracle. We remark that nonces used for the encryption queries can be used in its output.

For the $\mathrm{AEAD}_{Perm(\{0,1\}^n)}$ mode define

$$\mathbf{Adv}^{\mathrm{Auth}}_{\mathrm{AEAD}_{Perm(\{0,1\}^n)}}(\mathcal{A}) = \Pr\left[\pi \xleftarrow{\mathcal{U}} Perm(\{0,1\}^n) : \mathcal{A}^{\mathcal{E}} \text{ forges}\right],$$

where the probability is defined over the randomness of $\mathcal{A}$ and the choice of π.

Auxiliary security notions for MGM mode. For the $\mathrm{MGM}_{Perm(\{0,1\}^n)}$ mode we consider an auxiliary mPrivacy notion that extends the adversary's capabilities provided in the standard Privacy notion. While in the standard Privacy notion the nonce-respecting adversary makes a query (N, A, P), where $N \in \{0,1\}^{n-1}$, $A, P \in \{0,1\}^* : |A| + |P| > 0$, in the modified version the nonce-respecting adversary makes two sequential tied queries instead:

1. The first query consists of a nonce $N \in \{0,1\}^{n-1}$ and a parameter $l \in \mathbb{N}$ denoting the desired block-length of the response.

   In the case of the encryption oracle $\mathcal{E}$ the output is a tuple $\Gamma \in \{0,1\}^{n\times l}$ that consists of l blocks $\Gamma_k \in \{0,1\}^n$, $k = 1,\dots,l$, and is used for plaintext encryption in the MGM mode. In addition the oracle saves the N and l values that will be used for the next query processing.

   The first query processing:

$$\begin{cases} Y_1 = \pi(0\|N), & \\ Y_k = inc_r(Y_{k-1}), & 2 \leqslant k \leqslant l, \\ \Gamma_k = \pi(Y_k), & 1 \leqslant k \leqslant l. \end{cases}$$

   The random-bits oracle \$ returns the tuple $\Gamma \in \{0,1\}^{n\times l}$ that consists of l random blocks $\Gamma_k \xleftarrow{\mathcal{U}} \{0,1\}^n$.

2. The second query is a tuple $X \in \{0,1\}^{n\times l}$ that should consist of exactly l blocks $X_k \in \{0,1\}^n$, $k = 1,\dots,l$.

   In the case of the encryption oracle $\mathcal{E}$ this tuple is used as a direct input for the multilinear function of the MGM tag computation algorithm that also takes as input the nonce N from the previous query. In order to prevent trivial attacks we should introduce the following restriction on the tuple X: $X_l \neq 0^n$. This restriction follows from the presence of the mandatory non-zero block $\mathrm{str}_{n/2}(|A|)\|\mathrm{str}_{n/2}(|C|)$. As a response the encryption oracle returns a tag $T \in \{0,1\}^s$.

   The second query processing:

$$\begin{cases} Z_1 = \pi(1\|N), & \\ Z_k = inc_l(Z_{k-1}), & 2 \leqslant k \leqslant l, \\ H_k = \pi(Z_k), & 1 \leqslant k \leqslant l, \\ \tau = \displaystyle\sum_{k=1}^{l} H_k \cdot X_k, & \\ T = \mathrm{msb}_s(\pi(\tau)). & \end{cases}$$

The random-bits oracle \$ returns a random tag $T \overset{\mathcal{U}}{\leftarrow} \{0,1\}^s$.

Similarly we introduce an auxiliary mAuthenticity notion: queries to the encryption oracle $\mathcal{E}$ are modified in the same way as for the Privacy notion, and the output of an adversary is a message (N, X, T), where $N \in \{0,1\}^{n-1}$, $T \in \{0,1\}^s$, and $X \in \{0,1\}^{n\times *}$ is a tuple where the last block X_l is non-zero. Similarly, the adversary forges if (N, X, T) is a valid message and the value T was not returned by the encryption oracle as a response to the tied queries N and X.

Remark 5.1. For the $\mathrm{MGM}_{Func(\{0,1\}^n)}$ mode the auxiliary notions are defined in the same way except for the permutation $\pi \overset{\mathcal{U}}{\leftarrow} Perm(\{0,1\}^n)$ which is replaced by the function $\rho \overset{\mathcal{U}}{\leftarrow} Func(\{0,1\}^n)$.

It is easy to show (using the reduction) that the proposed modifications cover all adversary's capabilities considered in the standard security notions.

Proposition 5.1. *For any Privacy-breaking adversary $\mathcal{A}$ that makes at most q queries with the total length of plaintexts and associated data at most σ blocks, there exists an mPrivacy-breaking adversary $\mathcal{A}'$ such that*

$$\mathbf{Adv}^{\mathrm{Priv}}_{\mathrm{MGM}_{Perm(\{0,1\}^n)}}(\mathcal{A}) = \mathbf{Adv}^{\mathrm{mPriv}}_{\mathrm{MGM}_{Perm(\{0,1\}^n)}}(\mathcal{A}'),$$

where $\mathcal{A}'$ makes at most q couples of tied queries with the total value of X lengths at most $\sigma + q$ blocks.

Proof. Construct an adversary $\mathcal{A}'$ that breaks mPrivacy-security of the $\mathrm{MGM}_{Perm(\{0,1\}^n)}$ mode using the adversary $\mathcal{A}$. The $\mathcal{A}'$ is constructed as follows. The adversary $\mathcal{A}'$ starts the adversary $\mathcal{A}$, intercepts $\mathcal{A}$'s queries and processes them by itself. During queries processing the adversary «simulates» the oracle of the adversary $\mathcal{A}$ making the appropriate queries to its own oracle. Intercepting the query (N, A, P) from $\mathcal{A}$ the adversary $\mathcal{A}'$ makes the following couple of tied queries to its oracle. The first query consists of the nonce N and the length parameter $l = |A|_n + |P|_n + 1$. Receiving the tuple $\Gamma = (\Gamma_1, \ldots, \Gamma_l)$ as a response to this query the adversary $\mathcal{A}'$ forms the ciphertext $C = P \oplus \mathrm{msb}_{|P|}(\Gamma_1 \| \ldots \| \Gamma_{|P_n|})$. After that the adversary $\mathcal{A}'$ makes the second query — the tuple X that consists of the blocks of the string $A \| 0^{n-a} \| C \| 0^{n-c} \| (\mathrm{str}_{n/2}(|A|) \| \mathrm{str}_{n/2}(|C|))$. Note that the tuple X length is exactly l blocks. Receiving the tag T as a response to the second query the adversary $\mathcal{A}'$ returns the value (C, T) to the adversary $\mathcal{A}'$. As a result the adversary $\mathcal{A}'$ returns the result of $\mathcal{A}$.

Note that if the adversary $\mathcal{A}'$ interacts with the encryption oracle $\mathcal{E}$ defined by the mPrivacy notion, then it perfectly simulates for $\mathcal{A}$ the encryption oracle $\mathcal{E}$ defined by the Privacy notion, and if it interacts with the random-bits oracle \$, then it perfectly simulates $\mathcal{A}$'s random-bits oracle \$. Therefore, for such an adversary:

$$\mathbf{Adv}^{\mathrm{mPriv}}_{\mathrm{MGM}_{Perm(\{0,1\}^n)}}(\mathcal{A}') = \Pr\left[\pi \overset{\mathcal{U}}{\leftarrow} Perm(\{0,1\}^n) : (\mathcal{A}')^{\mathcal{E}} \Rightarrow 1\right] - \Pr\left[(\mathcal{A}')^{\$} \Rightarrow 1\right] =$$
$$= \Pr\left[\pi \overset{\mathcal{U}}{\leftarrow} Perm(\{0,1\}^n) : \mathcal{A}^{\mathcal{E}} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{\$} \Rightarrow 1\right] = \mathbf{Adv}^{\mathrm{Priv}}_{\mathrm{MGM}_{Perm(\{0,1\}^n)}}(\mathcal{A}).$$

Note that mPrivacy-breaking adversary $\mathcal{A}'$ makes queries with X length one more block larger than the total length of A and P in the initial query of $\mathcal{A}'$. Intercepting q queries with the total length of plaintexts and associated data at most σ blocks, $\mathcal{A}'$ makes at most q couples of tied queries with the total value of X lengths at most $\sigma + q$ blocks.

□

Proposition 5.2. *For any Authenticity-breaking adversary $\mathcal{A}$, that makes at most q encryption queries with the total length of plaintexts and associated data at most σ blocks and outputs a forgery with the summary length of ciphertext and associated data at most l blocks, there exists an mAuthenticity-breaking adversary $\mathcal{A}'$ such that*

$$\mathbf{Adv}^{\text{Auth}}_{\text{MGM}_{Perm(\{0,1\}^n)}}(\mathcal{A}) = \mathbf{Adv}^{\text{mAuth}}_{\text{MGM}_{Perm(\{0,1\}^n)}}(\mathcal{A}'),$$

where $\mathcal{A}'$ makes at most q couples of tied encryption queries with the total value of X lengths at most $\sigma + q$ blocks and outputs a forgery with the X length at most $l + 1$ blocks.

The proof of this proposition is same as proof of Proposition 5.1.

6 Security Bounds

Additional notation. For convenience we introduce the following notation:

- $\widetilde{Y}^i = (\widetilde{Y}^i_1, \dots, \widetilde{Y}^i_{l_i})$, $Y^i_k \in \{0,1\}^n$, — the tuple that consists of random function inputs used as counters during encryption for the i-th query.
- $\widetilde{Z}^i = (\widetilde{Z}^i_1, \dots, \widetilde{Z}^i_{l_i})$, $Z^i_k \in \{0,1\}^n$, — the tuple that consists of random function inputs used as counters during computation of multilinear function coefficients for the i-th query.
- $\widetilde{X}^i = (\widetilde{X}^i_1, \dots, \widetilde{X}^i_{l_i})$, $X^i_k \in \{0,1\}^n$, — the tuple that consists of message blocks in the i-th query.
- $\widetilde{\Gamma}^i = (\widetilde{\Gamma}^i_1, \dots, \widetilde{\Gamma}^i_{l_i})$, $\Gamma^i_k = \rho(Y^i_k) \in \{0,1\}^n$, — the tuple that consists of random function outputs used during encryption for the i-th query.
- $\widetilde{H}^i = (\widetilde{H}^i_1, \dots, \widetilde{H}^i_{l_i})$, $H^i_k = \rho(Z^i_k) \in \{0,1\}^n$, — the tuple that consists of random function outputs used as multilinear function coefficients for the i-th query.
- $\widetilde{\tau}_i = \sum_{j=1}^{l_i} \widetilde{H}^i_k \cdot \widetilde{X}^i_k$ — the output of multilinear function for the i-th query. Here the bit strings are interpreted as elements of $GF(2^n)$.
- $\widetilde{T}_i = \text{msb}_s(\rho(\widetilde{\tau}_i))$ — the tag value for the i-th query.
- $\widetilde{\mathbf{Dom}}^i = \left(0\|\widetilde{N}_1, 1\|\widetilde{N}_1, \widetilde{Y}^1_1, \widetilde{Z}^1_1, \dots, \widetilde{Y}^1_{l_1}, \widetilde{Z}^1_{l_1}, \widetilde{\tau}_1, \dots, 0\|\widetilde{N}_i, 1\|\widetilde{N}_i, \widetilde{Y}^i_1, \widetilde{Z}^i_1, \dots, \widetilde{Y}^i_{l_i}, \widetilde{Z}^i_{l_i}, \widetilde{\tau}_i\right)$ — the tuple that consists of all random variables used during processing of the first i queries.

6.1 mPrivacy-security of MGM mode

We consider the deterministic computationally unbounded adversary $\mathcal{A}$ that makes at most q couples of tied queries where the sum of the length parameter values for each query is at most σ blocks. The adversary is determined by $3q$ functions:

- q functions $l^{\mathcal{A}}_i$ that define the size parameters chosen by $\mathcal{A}$ for each query.

The first function $l_1^{\mathcal{A}}$ is constant, i.e. it is defined by the constant l_1, and the next functions are defined as follows:

$$l_i = l_i^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{i-1}, T_{i-1}) :$$
$$\underbrace{\{0,1\}^{n\times *} \times \{0,1\}^s \times \ldots \times \{0,1\}^{n\times *} \times \{0,1\}^s}_{i-1} \to \mathbb{N},\ i = 2, \ldots, q.$$

These functions must satisfy the following requirement:

$$\sum_{i=1}^{q} l_i^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{i-1}, T_{i-1}) = \sigma, \quad \forall\ \Gamma^1, T_1, \ldots, \Gamma^q, T_q.$$

- q functions $N_i^{\mathcal{A}}$ that define nonces chosen by $\mathcal{A}$ for each query.

  The function $N_1^{\mathcal{A}}$ is constant, i.e. it is defined by the constant N_1, and the next functions are defined as follows:

$$N_i = N_i^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{i-1}, T_{i-1}) :$$
$$\underbrace{\{0,1\}^{n\times *} \times \{0,1\}^s \times \ldots \times \{0,1\}^{n\times *} \times \{0,1\}^s}_{i-1} \to \{0,1\}^{n-1},\ i = 2, \ldots, q.$$

  These functions must satisfy the following requirement:

$$\forall\ 1 \leqslant i, j \leqslant q,\ i \neq j,\ \forall\ \Gamma^1, T_1, \ldots, \Gamma^q, T_q$$
$$N_i^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{i-1}, T_{i-1}) \neq N_j^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{j-1}, T_{i-1}).$$

- q functions $X_i^{\mathcal{A}}$ that define messages chosen by $\mathcal{A}$ for each query:

$$X^i = X_i^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{i-1}, T_{i-1}, \Gamma^i) :$$
$$\underbrace{\{0,1\}^{n\times *} \times \{0,1\}^s \times \ldots \times \{0,1\}^{n\times *} \times \{0,1\}^s}_{i-1} \times \{0,1\}^{n\times *} \to \{0,1\}^{n\times *},\ i = 1, \ldots, q.$$

  These functions must satisfy the following requirements:

$$\forall\ \Gamma^1, T_1, \ldots, \Gamma^{q-1}, T_{q-1}, \Gamma^q,\ X^i = X_i^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{i-1}, T_{i-1}, \Gamma^i) \in \{0,1\}^{n\times l_i},$$
$$l_i = l_i^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{i-1}, T_{i-1}) : X_{l_i}^i \neq 0^n\ \forall\ 1 \leqslant i \leqslant q.$$

Remark 6.1. Note that there is no need to completely define the considered above functions. Indeed, during the attack an adversary will obtain only the consistent responses Γ_i such that $\Gamma_i \in \{0,1\}^{m\times l_i}$, where $l_i = l_i^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{i-1}, T_{i-1})$.

Lemma 6.1. *For any* $\mathrm{MGM}_{Func(\{0,1\}^n)}$ *mPrivacy-breaking adversary $\mathcal{A}$, that makes at most q couples of tied queries with the total value of X lengths at most σ blocks, the following inequality holds:*

$$\Pr\left[\widetilde{\mathbf{Dom}}^q\ coll\right] \leqslant \frac{\sigma^2 + 8\sigma q + 3q^2}{2^n},$$

where the probability is defined over the choice of the function ρ uniformly chosen from the set $Func(\{0,1\}^n)$.

Proof. We have:

$$\Pr\left[\widetilde{\mathbf{Dom}}^{q}\ coll\right] = \Pr\left[\widetilde{\mathbf{Dom}}^{q}\ coll \cap \widetilde{\mathbf{Dom}}^{q-1}\ \overline{coll}\right] + \\ + \Pr\left[\widetilde{\mathbf{Dom}}^{q}\ coll \cap \widetilde{\mathbf{Dom}}^{q-1}\ coll\right] = \Pr\left[\widetilde{\mathbf{Dom}}^{q}\ coll \cap \widetilde{\mathbf{Dom}}^{q-1}\ \overline{coll}\right] + \\ + \Pr\left[\widetilde{\mathbf{Dom}}^{q-1}\ coll\right].$$

Note that for $\Pr\left[\widetilde{\mathbf{Dom}}^{q-1}\ coll\right]$ the same formula will be correct. Therefore, for the probability $\Pr\left[\widetilde{\mathbf{Dom}}^{q}\ coll\right]$ the following equality holds

$$\Pr\left[\widetilde{\mathbf{Dom}}^{q}\ coll\right] = \sum_{i=2}^{q} \Pr\left[\widetilde{\mathbf{Dom}}^{i}\ coll \cap \widetilde{\mathbf{Dom}}^{i-1}\ \overline{coll}\right] + \Pr\left[\widetilde{\mathbf{Dom}}^{1}\ coll\right].$$

Firstly consider the probability $\Pr\left[\widetilde{\mathbf{Dom}}^{1}\ coll\right]$.

$$\Pr\left[\widetilde{\mathbf{Dom}}^{1}\ coll\right] = \sum_{\substack{Y^1, Z^1: \\ \mathbf{Dom}^1 \setminus \{\widetilde{\tau}_1\}\ coll}} \Pr\left[\left\{\substack{\widetilde{Y^1} = Y^1 \\ \widetilde{Z^1} = Z^1}\right\}\right] + \sum_{\substack{Y^1, Z^1: \\ \mathbf{Dom}^1 \setminus \{\widetilde{\tau}_1\}\ \overline{coll}}} \Pr\left[\widetilde{\mathbf{Dom}}^{1}\ coll \cap \left\{\substack{\widetilde{Y^1} = Y^1 \\ \widetilde{Z^1} = Z^1}\right\}\right].$$

Consider the first summand.

$$\sum_{\substack{Y^1, Z^1: \\ \mathbf{Dom}^1 \setminus \{\widetilde{\tau}_1\}\ coll}} \Pr\left[\left\{\substack{\widetilde{Y^1} = Y^1 \\ \widetilde{Z^1} = Z^1}\right\}\right] = \sum_{\substack{Y^1, Z^1: \\ \mathbf{Dom}^1 \setminus \{\widetilde{\tau}_1\}\ coll}} \frac{\#\left\{\rho : \substack{\rho(0 \| N_1) = Y_1^1 \\ \rho(1 \| N_1) = Z_1^1}\right\}}{2^{n2^n}} = \\ = \sum_{\substack{Y^1, Z^1: \\ \mathbf{Dom}^1 \setminus \{\widetilde{\tau}_1\}\ coll}} \frac{1}{2^{2n}} = \#\left\{\substack{Y^1, Z^1: \\ \mathbf{Dom}^1 \setminus \{\widetilde{\tau}_1\}\ coll}\right\} \cdot \frac{1}{2^{2n}} \leqslant \\ \#\left(\bigcup_{b \in \{0,1\}} \left\{\substack{Y^1: \\ b \| N_1 \in Y^1}\right\} \times \left\{Z^1\right\} \cup \bigcup_{b \in \{0,1\}} \left\{\substack{Z^1: \\ b \| N_1 \in Z^1}\right\} \times \left\{Y^1\right\} \cup \left\{\substack{Y^1, Z^1: \\ Y^1 \cap Z^1 \neq \emptyset}\right\}\right) \cdot \frac{1}{2^{2n}} \leqslant \\ \leqslant (2l_1 \cdot 2^n + 2l_1 \cdot 2^n + l_1^2 \cdot 2^n) \cdot \frac{1}{2^{2n}} = \frac{4l_1 + l_1^2}{2^n}.$$

Consider the second summand. Note that after additional fixation of tuples Γ^1, H^1 the random variable $\widetilde{\tau}_1$ takes the fixed value $\tau_1 = \sum_{k_1=1}^{l_1} H_{k_1}^1 \cdot X_{k_1}^1$, where $X^1 = X_1^{\mathcal{A}}(\Gamma^1)$, $X_{l_1}^1 \neq 0^n$.

$$\sum_{\substack{Y^1,Z^1:\\ \mathbf{Dom}^1\setminus\{\widetilde{\tau}_1\}\ \overline{coll}}} \Pr\left[\widetilde{\mathbf{Dom}}^1\ coll \cap \left\{\substack{\widetilde{Y^1}=Y^1\\ \widetilde{Z^1}=Z^1}\right\}\right] = \sum_{\substack{Y^1,Z^1:\\ \mathbf{Dom}^1\setminus\{\widetilde{\tau}_1\}\ \overline{coll}}} \sum_{\substack{\Gamma^1,H^1:\\ \mathbf{Dom}^1\ coll}} \Pr\left[\left\{\substack{\widetilde{Y^1}=Y^1\\ \widetilde{Z^1}=Z^1}\right\} \cap \left\{\substack{\widetilde{\Gamma^1}=\Gamma^1\\ \widetilde{H^1}=H^1}\right\}\right] =$$

$$= \sum_{\substack{Y^1,Z^1:\\ \mathbf{Dom}^1\setminus\{\widetilde{\tau}_1\}\ \overline{coll}}} \sum_{\substack{\Gamma^1,H^1:\\ \mathbf{Dom}^1\ coll}} \frac{\#\left\{\rho : \substack{\rho(0\|N_1)=Y^1_1\\ \rho(1\|N_1)=Z^1_1}\ \substack{\rho(Y^1_{k_1})=\Gamma^1_{k_1}\\ \rho(Z^1_{k_1})=H^1_{k_1}}\ \ k_1=\overline{1,l_1}\right\}}{2^{n2^n}} = \sum_{\substack{Y^1,Z^1:\\ \mathbf{Dom}^1\setminus\{\widetilde{\tau}_1\}\ \overline{coll}}} \sum_{\substack{\Gamma^1,H^1:\\ \mathbf{Dom}^1\ coll}} \frac{1}{2^{n(2l_1+2)}} \leqslant$$

$$\leqslant \sum_{\substack{Y^1,Z^1:\\ \mathbf{Dom}^1\setminus\{\widetilde{\tau}_1\}\ \overline{coll}}} \sum_{\Gamma^1} \#\left\{\substack{H^1:\\ \mathbf{Dom}^1\ coll}\right\} \cdot \frac{1}{2^{n(2l_1+2)}} \leqslant$$

$$\leqslant \sum_{\substack{Y^1,Z^1:\\ \mathbf{Dom}^1\setminus\{\widetilde{\tau}_1\}\ \overline{coll}}} \sum_{\Gamma^1} \#\left(\bigcup_{b\in\{0,1\}} \left\{\substack{H^1:\\ \tau_1=b\|N_1}\right\} \cup \left\{\substack{H^1:\\ \tau_1\in Y^1}\right\} \cup \left\{\substack{H^1:\\ \tau_1\in Z^1}\right\}\right) \cdot \frac{1}{2^{n(2l_1+2)}} \leqslant$$

$$\leqslant \sum_{\substack{Y^1,Z^1:\\ \mathbf{Dom}^1\setminus\{\widetilde{\tau}_1\}\ \overline{coll}}} \sum_{\Gamma^1} \left(\sum_{b\in\{0,1\}} \underbrace{\#\left\{\substack{H^1:\\ \tau_1=b\|N_1}\right\}}_{=2^{nl_1-n}} + \underbrace{\#\left\{\substack{H^1:\\ \tau_1\in Y^1}\right\}}_{=l_1\cdot 2^{nl_1-n}} + \underbrace{\#\left\{\substack{H^1:\\ \tau_1\in Z^1}\right\}}_{=l_1\cdot 2^{nl_1-n}}\right) \cdot \frac{1}{2^{n(2l_1+2)}} \leqslant$$

$$\leqslant \underbrace{\#\left\{Y^1,Z^1\right\}}_{=2^{2n}} \cdot \underbrace{\#\left\{\Gamma^1\right\}}_{=2^{nl_1}} \cdot (2+l_1+l_1)\cdot 2^{nl_1-n} \cdot \frac{1}{2^{n(2l_1+2)}} \leqslant \frac{(2l_1+2)}{2^n}.$$

Thus,

$$\Pr\left[\widetilde{\mathbf{Dom}}^1\ coll\right] \leqslant \frac{4l_1+l_1^2}{2^n} + \frac{(2l_1+2)}{2^n} \leqslant \frac{l_1^2+6l_1+2}{2^n}.$$

Consider the probability $\Pr\left[\widetilde{\mathbf{Dom}}^i\ coll \cap \widetilde{\mathbf{Dom}}^{i-1}\ \overline{coll}\right],\ i=2,\dots,q.$

$$\Pr\left[\widetilde{\mathbf{Dom}}^i\ coll \cap \widetilde{\mathbf{Dom}}^{i-1}\ \overline{coll}\right] = \sum_{\substack{\Gamma^1,\dots,\Gamma^{i-1}\\ T_1,\dots,T^{i-1}}} \Pr\left[\widetilde{\mathbf{Dom}}^i\ coll \cap \widetilde{\mathbf{Dom}}^{i-1}\ \overline{coll} \cap \left\{\substack{\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j}\right\}_{j=1}^{i-1}\right].$$

Note that after fixation of the values $\Gamma^j, T_j,\ j=1,\dots,i-1$,

1. the random variables $\widetilde{l}_j$ take the fixed values $l_j = l_j^{\mathcal{A}}(\Gamma^1, T_1, \dots, \Gamma^{j-1}, T_{j-1})$, $j=1,\dots,i$.
2. in the tuple $\widetilde{\mathbf{Dom}}^i$ random variables $\widetilde{N}_j$ take the fixed values $N_j = N_j^{\mathcal{A}}(\Gamma^1, T_1, \dots, \Gamma^{j-1}, T_{j-1})$, $j=1,\dots,i$, similarly in the tuple $\widetilde{\mathbf{Dom}}^{i-1}$ the random variables $\widetilde{N}_1,\dots,\widetilde{N}_{i-1}$ takes the appropriate fixed values.
3. the random variables $\widetilde{X}^j$ takes the fixed values $X^j = X_j^{\mathcal{A}}(\Gamma^1, T_1, \dots, \Gamma^{j-1}, T_{j-1}, \Gamma^j)$, $j=1,\dots,i-1$.

Given these facts the following equality holds

$$\sum_{\substack{\Gamma^1,\ldots,\Gamma^{i-1}\\ T_1,\ldots,T^{i-1}}} \Pr\left[\widetilde{\mathbf{Dom}}^{i}\ coll \cap \widetilde{\mathbf{Dom}}^{i-1}\ \overline{coll} \cap \left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^{i-1}\right] =$$

$$= \sum_{\substack{\Gamma^1,\ldots,\Gamma^{i-1}\\ T_1,\ldots,T^{i-1}}} \sum_{\substack{Y^1,\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{i-1}\\ H^1,\ldots,H^{i-1}:\\ \mathbf{Dom}^{i-1}\ \overline{coll}}} \Pr\left[\widetilde{\mathbf{Dom}}^{i}\ coll \cap \left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^{i-1} \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j\end{smallmatrix}\right\}_{j=1}^{i-1}\right].$$

Note that after additional fixation of tuples $H^j,\ j=1,\ldots,i-1$, in the tuple $\widetilde{\mathbf{Dom}}^{i-1}$ the random variables $\widetilde{\tau}_j$ take the fixed values $\tau_j=\sum_{k_j=1}^{l_j} H^j_{k_j}\cdot X^j_{k_j}$, $j=1,\ldots,i-1$.

The considered sum can be divided into two subsums:

$$\underbrace{\sum_{\substack{\Gamma^1,\ldots,\Gamma^{i-1}\\ T_1,\ldots,T_{i-1}}} \sum_{\substack{Y^1,\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{i-1}\\ H^1,\ldots,H^{i-1}:\\ \mathbf{Dom}^{i-1}\ \overline{coll}\\ 0\|N_i\vee 1\|N_i\in\mathbf{Dom}^{i-1}}} \Pr\left[\left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^{i-1} \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j\end{smallmatrix}\right\}_{j=1}^{i-1}\right]}_{sum_1} +$$

$$+\underbrace{\sum_{\substack{\Gamma^1,\ldots,\Gamma^{i-1}\\ T_1,\ldots,T_{i-1}}} \sum_{\substack{Y^1,\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{i-1}\\ H^1,\ldots,H^{i-1}:\\ \mathbf{Dom}^{i-1}\ \overline{coll}\\ 0\|N_i,1\|N_i\notin\mathbf{Dom}^{i-1}}} \Pr\left[\widetilde{\mathbf{Dom}}^{i}\ coll \cap \left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^{i-1} \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j\end{smallmatrix}\right\}_{j=1}^{i-1}\right]}_{sum_2}.$$

Consider the first summand sum_1.

$$sum_1 = \sum_{\substack{\Gamma^1,\ldots,\Gamma^{i-1}\\ T_1,\ldots,T_{i-1}}} \sum_{\substack{Y^1,\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{i-1}\\ H^1,\ldots,H^{i-1}:\\ \mathbf{Dom}^{i-1}\ \overline{coll}\\ 0\|N_i\vee 1\|N_i\in\mathbf{Dom}^{i-1}}} \frac{\#\left\{\rho :\ \begin{smallmatrix} \rho(0\|N_j)=Y_1^j & \rho(Y^j_{k_j})=\Gamma^j_{k_j} & j=\overline{1,i-1}\\ \rho(1\|N_j)=Z_1^j & \rho(Z^j_{k_j})=H^j_{k_j} & k_j=\overline{1,l_j}\\ \mathrm{msb}_s(\rho(\tau_j))=T_j & & \end{smallmatrix}\right\}}{2^{n2^n}} =$$

$$= \sum_{\substack{\Gamma^1,\ldots,\Gamma^{i-1}\\ T_1,\ldots,T_{i-1}}} \sum_{\substack{Y^1,\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{i-1}\\ H^1,\ldots,H^{i-1}:\\ \mathbf{Dom}^{i-1}\ \overline{coll}\\ 0\|N_i\vee 1\|N_i\in\mathbf{Dom}^{i-1}}} \frac{2^{n(2^n-\sum_{j=1}^{i-1}(2l_j+3))}\cdot 2^{(n-s)(i-1)}}{2^{n2^n}} \leqslant$$

$$\leqslant \sum_{\substack{\Gamma^1,\ldots,\Gamma^{i-1}\\ T_1,\ldots,T_{i-1}}} \underbrace{\#\left\{\begin{smallmatrix} Y^1,\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{i-1}\\ H^1,\ldots,H^{i-1}:\\ 0\|N_i\vee 1\|N_i\in\mathbf{Dom}^{i-1}\end{smallmatrix}\right\}}_{A} \cdot \frac{1}{2^{n\sum_{j=1}^{i-1}(2l_j+2)+s(i-1)}}.$$

Estimate the cardinality of the set A for the fixed values Γ^j, T_j, $j=1,\ldots,i-1$ (consequently, for the fixed values N_j, X^j, $j=1,\ldots,i-1$, and N_i). The set A can be covered by the union of the following sets:

$$A \subset \bigcup_{b\in\{0,1\}} \bigcup_{j=1}^{i-1} \Bigg(\left\{\begin{smallmatrix} Y^j:\\ b\|N_i\in Y^j\end{smallmatrix}\right\} \times \left\{\begin{smallmatrix} Y^1,\ldots,Y^{j-1},Y^{j+1},\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{i-1}\\ H^1,\ldots,H^{i-1}\end{smallmatrix}\right\} \cup \left\{\begin{smallmatrix} Z^j:\\ b\|N_i\in Z^j\end{smallmatrix}\right\} \times \left\{\begin{smallmatrix} Y^1,\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{j-1},Z^{j+1},\ldots,Z^{i-1}\\ H^1,\ldots,H^{i-1}\end{smallmatrix}\right\} \cup$$

$$\cup \left\{\begin{smallmatrix} H^j:\\ b\|N_i=\tau_j\end{smallmatrix}\right\} \times \left\{\begin{smallmatrix} Y^1,\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{i-1}\\ H^1,\ldots,H^{j-1},H^{j+1},\ldots,H^{i-1}\end{smallmatrix}\right\} \Bigg).$$

Thus the cardinality of the set A can be estimated in the following way:

$$\#A \leqslant \sum_{b\in\{0,1\}} \sum_{j=1}^{i-1} \Big(\underbrace{\#\left\{Y^j : b\|N_i \in Y^j\right\}}_{=l_j} \cdot 2^{n\sum_{t=1}^{i-1}(l_t+2)-n} +$$

$$+ \underbrace{\#\left\{Z^j : b\|N_i \in Z^j\right\}}_{=l_j} \cdot 2^{n\sum_{t=1}^{i-1}(l_t+2)-n} + \underbrace{\#\left\{H^j : b\|N_i = \tau_j\right\}}_{=2^{nl_j-n}} \cdot 2^{n\sum_{t=1}^{i-1}(l_t+2)-nl_j} \Big) =$$

$$= \underbrace{\left(\sum_{j=1}^{i-1}(4l_j+2)\right)}_{\omega_1} \cdot 2^{n\sum_{j=1}^{i-1}(l_j+2)-n},\ \ \forall \Gamma^1, T_1, \ldots, \Gamma^{i-1}, T_{i-1}.$$

Thus,

$$sum_1 \leqslant \sum_{\substack{\Gamma^1,\dots,\Gamma^{i-1}\\ T_1,\dots,T_{i-1}}} \omega_1 \cdot 2^{n\sum_{j=1}^{i-1}(l_j+2)-n} \cdot \frac{1}{2^{n\sum_{j=1}^{i-1}(2l_j+2)+s(i-1)}} = \#\left\{\substack{\Gamma^1,\dots,\Gamma^{i-1}\\ T_1,\dots,T_{i-1}}\right\} \cdot \frac{\omega_1}{2^{n\sum_{j=1}^{i-1}l_j+n+s(i-1)}} =$$

$$= 2^{n\sum_{j=1}^{i-1}l_j} \cdot 2^{s(i-1)} \cdot \frac{\omega_1}{2^{n\sum_{j=1}^{i-1}l_j+n+s(i-1)}} = \frac{\omega_1}{2^n}.$$

Consider the second summand sum_2.

$$sum_2 = \underbrace{\sum_{\substack{\Gamma^1,\dots,\Gamma^{i-1}\\ T_1,\dots,T_{i-1}}} \sum_{\substack{Y^1,\dots,Y^{i-1}\\ Z^1,\dots,Z^{i-1}\\ H^1,\dots,H^{i-1}:\\ \mathbf{Dom}^{i-1}\ \overline{coll}\\ 0\|N_i,1\|N_i\notin\mathbf{Dom}^{i-1}}} \sum_{\substack{Y^i,Z^i:\\ \mathbf{Dom}^i\setminus\{\widetilde{\tau}_i\}\ coll}} \Pr\left[\left\{\substack{\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j}\right\}_{j=1}^{i-1} \cap \left\{\substack{\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j}\right\}_{j=1}^{i-1} \cap \left\{\substack{\widetilde{Y}^i=Y^i\\ \widetilde{Z}^i=Z^i}\right\}\right] +}_{sum_2^1}$$

$$\underbrace{+\sum_{\substack{\Gamma^1,\dots,\Gamma^{i-1}\\ T_1,\dots,T_{i-1}}} \sum_{\substack{Y^1,\dots,Y^{i-1}\\ Z^1,\dots,Z^{i-1}\\ H^1,\dots,H^{i-1}:\\ \mathbf{Dom}^{i-1}\ \overline{coll}\\ 0\|N_i,1\|N_i\notin\mathbf{Dom}^{i-1}}} \sum_{\substack{Y^i,Z^i:\\ \mathbf{Dom}^i\setminus\{\widetilde{\tau}_i\}\ \overline{coll}}} \Pr\left[\widetilde{\mathbf{Dom}}^i\ coll \cap \left\{\substack{\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j}\right\}_{j=1}^{i-1} \cap \left\{\substack{\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j}\right\}_{j=1}^{i-1} \cap \left\{\substack{\widetilde{Y}^i=Y^i\\ \widetilde{Z}^i=Z^i}\right\}\right]}_{sum_2^2}.$$

Consider the summand sum_2^1.

$$sum_2^1 = \sum_{\substack{\Gamma^1,\dots,\Gamma^{i-1}\\ T_1,\dots,T_{i-1}}} \sum_{\substack{Y^1,\dots,Y^{i-1}\\ Z^1,\dots,Z^{i-1}\\ H^1,\dots,H^{i-1}:\\ \mathbf{Dom}^{i-1}\ \overline{coll}\\ 0\|N_i,1\|N_i\notin\mathbf{Dom}^{i-1}}} \sum_{\substack{Y^i,Z^i:\\ \mathbf{Dom}^i\setminus\{\widetilde{\tau}_i\}\ coll}} \frac{\#\left\{\rho : \begin{array}{ccc} \rho(0\|N_j)=Y_1^j & \rho(Y_{k_j}^j)=\Gamma_{k_j}^j & \\ \rho(1\|N_j)=Z_1^j & & j=\overline{1,i-1}, \\ & \rho(Z_{k_j}^j)=H_{k_j}^j & k_j=\overline{1,l_j} \\ \rho(0\|N_i)=Y_1^i & & \\ \rho(1\|N_i)=Z_1^i & \mathrm{msb}_s(\rho(\tau_j))=T_j & \end{array}\right\}}{2^{n2^n}} =$$

$$= \sum_{\substack{\Gamma^1,\dots,\Gamma^{i-1}\\ T_1,\dots,T_{i-1}}} \sum_{\substack{Y^1,\dots,Y^{i-1}\\ Z^1,\dots,Z^{i-1}\\ H^1,\dots,H^{i-1}:\\ \mathbf{Dom}^{i-1}\ \overline{coll}\\ 0\|N_i\vee 1\|N_i\in\mathbf{Dom}^{i-1}}} \sum_{\substack{Y^i,Z^i:\\ \mathbf{Dom}^i\setminus\{\widetilde{\tau}_i\}\ coll}} \frac{2^{n(2^n-\sum_{j=1}^{i-1}(2l_j+3)-2)} \cdot 2^{(n-s)(i-1)}}{2^{n2^n}} \leqslant$$

$$\leqslant \sum_{\substack{\Gamma^1,\dots,\Gamma^{i-1}\\ T_1,\dots,T_{i-1}}} \sum_{\substack{Y^1,\dots,Y^{i-1}\\ Z^1,\dots,Z^{i-1}\\ H^1,\dots,H^{i-1}:\\ \mathbf{Dom}^{i-1}\ \overline{coll}\\ 0\|N_i,1\|N_i\notin\mathbf{Dom}^{i-1}}} \#\underbrace{\left\{\substack{Y^i,Z^i:\\ \mathbf{Dom}^i\setminus\{\widetilde{\tau}_i\}\ coll}\right\}}_{B} \cdot \frac{1}{2^{n\sum_{j=1}^{i-1}(2l_j+2)+2n+s(i-1)}}.$$

Estimate the cardinality of the set B for the fixed values $\Gamma^j, T_j, Y^j, Z^j, H^j$, $j = 1, \ldots, i-1$ (consequently, for the fixed value N_i and for all fixed values from $\mathbf{Dom}^{i-1}$). The set B can be covered by the union of the following sets:

$$B \subset \bigcup_{j=1}^{i-1} \left(\left\{ \substack{Z^i: \\ Z^i \cap Z^j \neq \emptyset} \right\} \cup \left\{ \substack{Z^i: \\ \tau_j \in Z^i} \right\} \right) \times \left\{ Y^i \right\} \quad \cup \quad \bigcup_{j=1}^{i-1} \left(\left\{ \substack{Y^i: \\ Y^i \cap Y^j \neq \emptyset} \right\} \cup \left\{ \substack{Y^i: \\ \tau_j \in Y^i} \right\} \right) \times \left\{ Z^i \right\} \quad \cup$$

$$\cup \quad \bigcup_{j=1}^{i-1} \bigcup_{k_j=1}^{l_j} \left(\left\{ \substack{Z^i: \\ Y^j_{k_j} \in Z^i} \right\} \times \left\{ Y^i \right\} \cup \left\{ \substack{Y^i: \\ Z^j_{k_j} \in Y^i} \right\} \times \left\{ Z^i \right\} \right) \quad \cup$$

$$\cup \quad \bigcup_{j=1}^{i} \bigcup_{b \in \{0,1\}} \left(\left\{ \substack{Z^i: \\ b \| N_j \in Z^i} \right\} \times \left\{ Y^i \right\} \cup \left\{ \substack{Y^i: \\ b \| N_i \in Y^i} \right\} \times \left\{ Z^i \right\} \right) \quad \cup \quad \left\{ \substack{Y^i, Z^i: \\ Y^i \cap Z^i \neq \emptyset} \right\}.$$

Thus the cardinality of the set B can be estimated in the following way:

$$\#B \leqslant \sum_{j=1}^{i-1} \Big(\underbrace{\# \left\{ Z^i : Z^i \cap Z^j \neq \emptyset \right\}}_{=(l_i + l_j - 1)} + \underbrace{\# \left\{ Z^i : \tau_j \in Z^i \right\}}_{=l_i} \Big) \cdot 2^n + \sum_{j=1}^{i-1} \Big(\underbrace{\# \left\{ Y^i : Y^i \cap Y^j \neq \emptyset \right\}}_{=(l_i + l_j - 1)} + \underbrace{\# \left\{ Y^i : \tau_j \in Y^i \right\}}_{=l_i} \Big) \cdot 2^n +$$

$$+ \sum_{j=1}^{i-1} \sum_{k_j=1}^{l_j} \Big(\underbrace{\# \left\{ Z^i : Y^j_{k_j} \in Z^i \right\}}_{=l_i} \cdot 2^n + \underbrace{\# \left\{ Y^i : Z^j_{k_j} \in Y^i \right\}}_{=l_i} \cdot 2^n \Big) +$$

$$+ \sum_{j=1}^{i} \sum_{b \in \{0,1\}} \Big(\underbrace{\# \left\{ Z^i : b \| N_j \in Z^i \right\}}_{=l_i} \cdot 2^n + \underbrace{\# \left\{ Y^i : b \| N_j \in Y^i \right\}}_{=l_i} \cdot 2^n \Big) + \sum_{Z_i} \underbrace{\# \left\{ Y^i : Y^i \cap Z^i \neq \emptyset \right\}}_{l_i^2} =$$

$$= \sum_{j=1}^{i-1} (4l_i + 2l_j - 2 + 2l_i l_j) \cdot 2^n + 4il_i \cdot 2^n + l_i^2 \cdot 2^n =$$

$$= \underbrace{\left(\sum_{j=1}^{i-1} (4l_i + 2l_j + 2l_i l_j - 2) + 4il_i + l_i^2 \right)}_{\omega_2^1} \cdot 2^n, \ \forall \ \Gamma^j, T_j, Y^j, Z^j, H^j, \ j = 1, \ldots, i-1.$$

Therefore,

$$sum_2^1 \leqslant \sum_{\substack{\Gamma^1, \ldots, \Gamma^{i-1} \\ T_1, \ldots, T_{i-1}}} \quad \sum_{\substack{Y^1, \ldots, Y^{i-1} \\ Z^1, \ldots, Z^{i-1} \\ H^1, \ldots, H^{i-1}: \\ \mathbf{Dom}^{i-1} \ \overline{coll} \\ 0 \| N_i, 1 \| N_i \notin \mathbf{Dom}^{i-1}}} \quad \omega_2^1 \cdot 2^n \cdot \frac{1}{2^{n \sum_{j=1}^{i-1} (2l_j + 2) + 2n + s(i-1)}} \leqslant$$

$$\leqslant \# \left\{ \substack{\Gamma^1, \ldots, \Gamma^{i-1} \\ T_1, \ldots, T_{i-1}} \right\} \cdot \# \left\{ \substack{Y^1, \ldots, Y^{i-1} \\ Z^1, \ldots, Z^{i-1} \\ H^1, \ldots, H^{i-1}} \right\} \cdot \frac{\omega_2^1}{2^{n \sum_{j=1}^{i-1} (2l_j + 2) + n + s(i-1)}} =$$

$$= 2^{n \sum_{j=1}^{i-1} l_j} \cdot 2^{s(i-1)} \cdot 2^{n \sum_{j=1}^{i-1} (l_j + 2)} \cdot \frac{\omega_2^1}{2^{n \sum_{j=1}^{i-1} (2l_j + 2) + n + s(i-1)}} = \frac{\omega_2^1}{2^n}.$$

Consider the summand sum_2^2.

$$sum_2^2 = \sum_{\substack{\Gamma^1,\dots,\Gamma^{i-1}\\ T_1,\dots,T_{i-1}}} \sum_{\substack{Y^1,\dots,Y^{i-1}\\ Z^1,\dots,Z^{i-1}\\ H^1,\dots,H^{i-1}:\\ \mathbf{Dom}^{i-1}\ \overline{coll}\\ 0\|N_i,1\|N_i\notin\mathbf{Dom}^{i-1}}} \sum_{\substack{Y^i,Z^i:\\ \mathbf{Dom}^i\setminus\{\widetilde{\tau}_i\}\ \overline{coll}}} \sum_{\substack{\Gamma^i,H^i:\\ \mathbf{Dom}^i\ coll}} \Pr\left[\left\{ \substack{\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j} \right\}_{j=1}^{i-1} \cap \left\{ \substack{\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j} \right\}_{j=1}^{i} \cap \left\{\widetilde{\Gamma}^i=\Gamma^i\right\} \right]$$

Note that after additional fixation of the values Γ^i, H^i the random variables $\widetilde{\tau}_i$ takes the fixed values $\tau_i = \sum_{k_i=1}^{l_i} H^i_{k_i} \cdot X^i_{k_i}$, где $X^i = X_i^{\mathcal{A}}(\Gamma^1, T_1, \dots, \Gamma^{i-1}, T_{i-1}, \Gamma^i)$.

Therefore,

$$sum_2^2 = \sum_{\substack{\Gamma^1,\dots,\Gamma^{i-1}\\ T_1,\dots,T_{i-1}}} \sum_{\substack{Y^1,\dots,Y^{i-1}\\ Z^1,\dots,Z^{i-1}\\ H^1,\dots,H^{i-1}:\\ \mathbf{Dom}^{i-1}\ \overline{coll}\\ 0\|N_i,1\|N_i\notin\mathbf{Dom}^{i-1}}} \sum_{\substack{Y^i,Z^i:\\ \mathbf{Dom}^i\setminus\{\widetilde{\tau}_i\}\ \overline{coll}}} \sum_{\substack{\Gamma^i,H^i:\\ \mathbf{Dom}^i\ coll}} \frac{\#\left\{ \rho : \substack{\rho(0\|N_j)=Y^j_1\\ \rho(1\|N_j)=Z^j_1,\\ \rho(Y^j_{k_j})=\Gamma^j_{k_j}\\ \rho(Z^j_{k_j})=H^j_{k_j}}, \ \substack{j=\overline{1,i},\\ k_j=\overline{1,l_j},} \ \ \substack{\mathrm{msb}_s(\rho(\tau_j))=T_j\\ j=\overline{1,i-1}} \right\}}{2^{n2^n}} =$$

$$= \sum_{\substack{\Gamma^1,\dots,\Gamma^{i-1}\\ T_1,\dots,T_{i-1}}} \sum_{\substack{Y^1,\dots,Y^{i-1}\\ Z^1,\dots,Z^{i-1}\\ H^1,\dots,H^{i-1}:\\ \mathbf{Dom}^{i-1}\ \overline{coll}\\ 0\|N_i,1\|N_i\notin\mathbf{Dom}^{i-1}}} \sum_{\substack{Y^i,Z^i:\\ \mathbf{Dom}^i\setminus\{\widetilde{\tau}_i\}\ \overline{coll}}} \sum_{\substack{\Gamma^i,H^i:\\ \mathbf{Dom}^i\ coll}} \frac{2^{n(2^n-\sum_{j=1}^{i-1}(2l_j+3)-(2l_i+2))} \cdot 2^{(n-s)(i-1)}}{2^{n2^n}} \leqslant$$

$$\leqslant \sum_{\substack{\Gamma^1,\dots,\Gamma^{i-1}\\ T_1,\dots,T_{i-1}}} \sum_{\substack{Y^1,\dots,Y^{i-1}\\ Z^1,\dots,Z^{i-1}\\ H^1,\dots,H^{i-1}:\\ \mathbf{Dom}^{i-1}\ \overline{coll}\\ 0\|N_i,1\|N_i\notin\mathbf{Dom}^{i-1}}} \sum_{\substack{Y^i,Z^i:\\ \mathbf{Dom}^i\setminus\{\widetilde{\tau}_i\}\ \overline{coll}}} \#\underbrace{\left\{ \substack{\Gamma^i,H^i:\\ \mathbf{Dom}^i\ coll} \right\}}_{C} \cdot \frac{1}{2^{n\sum_{j=1}^{i-1}(2l_j+2)+n(2l_i+2)+s(i-1)}}.$$

Estimate the cardinality of the set C for the fixed values $\Gamma^j, T_j, Y^j, Z^j, H^j$, $j = 1, \dots, i-1$ (consequently, for the fixed value N_i and all values from $\mathbf{Dom}^{i-1}$), Y^i, Z^i. The set C can be covered by the union of the following sets:

$$C \subset \bigcup_{\Gamma^i} \left(\left\{ \substack{H^i:\\ \tau_i\in\mathbf{Dom}^{i-1}} \right\} \cup \left\{ \substack{H^i:\\ \tau_i\in Z^i} \right\} \cup \left\{ \substack{H^i:\\ \tau_i\in Y^i} \right\} \cup \bigcup_{b\in\{0,1\}} \left\{ \substack{H^i:\\ \tau_i=b\|N_i} \right\} \right).$$

Thus the cardinality of the set C can be estimated in the following way:

$$\#C \leqslant \sum_{\Gamma^i} \Bigg(\underbrace{\#\left\{\substack{H^i:\\ \tau_i \in \mathbf{Dom}^{i-1}}\right\}}_{=\sum_{j=1}^{i-1}(2l_j+3)\cdot 2^{nl_i-n}} + \underbrace{\#\left\{\substack{H^i:\\ \tau_i \in Z^i}\right\}}_{=l_i\cdot 2^{nl_i-n}} + \underbrace{\#\left\{\substack{H^i:\\ \tau_i \in Y^i}\right\}}_{=l_i\cdot 2^{nl_i-n}} + \sum_{b\in\{0,1\}} \underbrace{\#\left\{\substack{H^i:\\ \tau_i = b\|N_i}\right\}}_{2^{nl_i-n}} \Bigg) =$$

$$= \sum_{j=1}^{i-1}(2l_j+3)\cdot 2^{2nl_i-n} + (2l_i+2)\cdot 2^{2nl_i-n} =$$

$$= \underbrace{\left(\sum_{j=1}^{i-1}(2l_j+3) + (2l_i+2)\right)}_{\omega_2^2} \cdot 2^{2nl_i-n},\ \forall\ \Gamma^j, T_j, Y^j, Z^j, H^j,\ j=\overline{1,i-1}, Y^i, Z^i.$$

Thus,

$$sum_2^2 \leqslant \sum_{\substack{\Gamma^1,\ldots,\Gamma^{i-1}\\ T_1,\ldots,T_{i-1}}} \sum_{\substack{Y^1,\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{i-1}\\ H^1,\ldots,H^{i-1}:\\ \mathbf{Dom}^{i-1}\ \overline{coll}\\ 0\|N_i,1\|N_i\notin\mathbf{Dom}^{i-1}}} \sum_{\substack{Y^i,Z^i:\\ \mathbf{Dom}^i\setminus\{\widetilde{\tau}_i\}\ \overline{coll}}} \frac{\omega_2^2\cdot 2^{2nl_i-n}}{2^{n\sum_{j=1}^{i-1}(2l_j+2)+n(2l_i+2)+s(i-1)}} \leqslant$$

$$\leqslant \#\left\{\substack{\Gamma^1,\ldots,\Gamma^{i-1}\\ T_1,\ldots,T_{i-1}}\right\}\cdot\#\left\{\substack{Y^1,\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{i-1}\\ H^1,\ldots,H^{i-1}}\right\}\cdot\#\left\{Y^i,Z^i\right\}\cdot\frac{\omega_2^2}{2^{n\sum_{j=1}^{i-1}(2l_j+2)+3n+s(i-1)}} =$$

$$= 2^{n\sum_{j=1}^{i-1}l_j}\cdot 2^{s(i-1)}\cdot 2^{n\sum_{j=1}^{i-1}(l_j+2)}\cdot 2^{2n}\cdot\frac{\omega_2^2}{2^{n\sum_{j=1}^{i-1}(2l_j+2)+3n+s(i-1)}} = \frac{\omega_2^2}{2^n}.$$

$$\Pr\left[\widetilde{\mathbf{Dom}}^i\ coll \cap \widetilde{\mathbf{Dom}}^{i-1}\ \overline{coll}\right] = sum_1 + sum_2^1 + sum_2^2 \leqslant \frac{\omega_1+\omega_2^1+\omega_2^2}{2^n} \leqslant$$

$$\leqslant \frac{\sum_{j=1}^{i-1}(4l_j+2)}{2^n} + \frac{\sum_{j=1}^{i-1}(4l_i+2l_j+2l_il_j-2)+4il_i+l_i^2}{2^n} + \frac{\sum_{j=1}^{i-1}(2l_j+3)+(2l_i+2)}{2^n} =$$

$$= \frac{2l_i\sum_{j=1}^{i-1}l_j + l_i^2 + 8\sum_{j=1}^{i-1}l_j + 8il_i + 3i - 2l_i - 1}{2^n} \leqslant$$

$$\leqslant \frac{2l_i\sum_{j=1}^{i-1}l_j + l_i^2 + 8\sum_{j=1}^{i-1}l_j + 8il_i + 3i}{2^n},\ i=2,\ldots,q.$$

Therefore,

$$\Pr\left[\widetilde{\mathbf{Dom}}^{q}\ coll\right] = \sum_{i=2}^{q} \Pr\left[\widetilde{\mathbf{Dom}}^{i}\ coll \cap \widetilde{\mathbf{Dom}}^{i-1}\ \overline{coll}\right] + \Pr\left[\widetilde{\mathbf{Dom}}^{1}\ coll\right] \leqslant$$

$$\leqslant \sum_{i=2}^{q} \frac{2l_i\sum_{j=1}^{i-1} l_j + l_i^2 + 8\sum_{j=1}^{i-1} l_j + 8il_i + 3i}{2^n} + \frac{l_1^2 + 6l_1 + 2}{2^n} \leqslant \left|\sum_{j=1}^{i-1} l_j = 0\ for\ i = 1\right| \leqslant$$

$$\leqslant \sum_{i=1}^{q} \frac{2l_i\sum_{j=1}^{i-1} l_j + l_i^2 + 8\sum_{j=1}^{i-1} l_j + 8il_i + 3i}{2^n} =$$

$$= \sum_{i=1}^{q} \frac{2l_i\sum_{j=1}^{i-1} l_j + l_i^2}{2^n} + \sum_{i=1}^{q} \frac{8\sum_{j=1}^{i-1} l_j + 8il_i}{2^n} + \sum_{i=1}^{q} \frac{3i}{2^n} \leqslant$$

$$\leqslant \frac{\sigma^2}{2^n} + \sum_{i=1}^{q} \frac{8(q-i)l_i + 8il_i}{2^n} + \frac{3q^2}{2^n} = \frac{\sigma^2 + 8\sigma q + 3q^2}{2^n}.$$

□

Lemma 6.2 ([3] PRP/PRF switching lemma)**.** *For any block cipher E and any adversary $\mathcal{A}$ making at most q' queries we have*

$$\mathbf{Adv}_{E}^{\mathrm{PRF}}(\mathcal{A}) \leqslant \mathbf{Adv}_{E}^{\mathrm{PRP\text{-}CPA}}(\mathcal{A}) + \frac{q'(q'-1)}{2^{n+1}}$$

Corollary 6.3. *For any adversary $\mathcal{A}$ making at most q' queries we have*

$$\mathbf{Adv}_{Perm(\{0,1\}^n)}^{\mathrm{PRF}}(\mathcal{A}) \leqslant \frac{(q')^2}{2^{n+1}}.$$

Theorem 6.4. *For any mPrivacy-breaking adversary $\mathcal{A}$, that makes q couples of tied queries with the total value of X lengths at most σ blocks, the following inequality holds*

$$\mathbf{Adv}_{\mathrm{MGM}_{Perm(\{0,1\}^n)}}^{\mathrm{mPriv}}(\mathcal{A}) \leqslant \frac{3(\sigma+3q)^2}{2^n}$$

Proof. Construct an adversary $\mathcal{A}'$ that breaks PRF-security of the cipher $Perm(\{0,1\}^n)$ using the adversary $\mathcal{A}$. The $\mathcal{A}'$ is constructed as follows. The adversary $\mathcal{A}'$ starts the adversary $\mathcal{A}$, intercepts $\mathcal{A}$'s queries and processes them by itself. During queries processing the adversary «simulates» the encryption oracle $\mathcal{E}$: implements the oracle functionality according to the definition of the mPrivacy notion, making the appropriate queries to its own oracle (random permutation π or random function ρ) for each block processing. Note that if the adversary $\mathcal{A}'$ interacts with the oracle π, then it simulates for $\mathcal{A}$ the encryption oracle $\mathcal{E}$ for the $\mathrm{MGM}_{Perm(\{0,1\}^n)}$ mode, and if it interacts with the oracle ρ, then it implements the encryption oracle $\mathcal{E}$ for the $\mathrm{MGM}_{Func(\{0,1\}^n)}$ mode. As a result the adversary $\mathcal{A}'$ returns the result of $\mathcal{A}$. For such an adversary:

$$\begin{aligned}
&\mathbf{Adv}^{\mathrm{PRF}}_{Perm(\{0,1\}^n)}(\mathcal{A}') = \\
&\quad = \Pr\left[\pi \overset{\mathcal{U}}{\leftarrow} Perm(\{0,1\}^n) : (\mathcal{A}')^{\pi} \Rightarrow 1\right] - \Pr\left[\rho \overset{\mathcal{U}}{\leftarrow} Func(\{0,1\}^n) : (\mathcal{A}')^{\rho} \Rightarrow 1\right] = \\
&\quad = \Pr\left[\pi \overset{\mathcal{U}}{\leftarrow} Perm(\{0,1\}^n) : \mathcal{A}^{\mathcal{E}} \Rightarrow 1\right] - \Pr\left[\rho \overset{\mathcal{U}}{\leftarrow} Func(\{0,1\}^n) : \mathcal{A}^{\mathcal{E}} \Rightarrow 1\right] = \\
&\quad = \left(\Pr\left[\pi \overset{\mathcal{U}}{\leftarrow} Perm(\{0,1\}^n) : \mathcal{A}^{\mathcal{E}} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{\$} \Rightarrow 1\right]\right) - \\
&\quad - \left(\Pr\left[\rho \overset{\mathcal{U}}{\leftarrow} Func(\{0,1\}^n) : \mathcal{A}^{\mathcal{E}} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{\$} \Rightarrow 1\right]\right) = \\
&\quad = \mathbf{Adv}^{\mathrm{mPriv}}_{\mathrm{MGM}_{Perm(\{0,1\}^n)}}(\mathcal{A}) - \mathbf{Adv}^{\mathrm{mPriv}}_{\mathrm{MGM}_{Func(\{0,1\}^n)}}(\mathcal{A}).
\end{aligned}$$

By the law of total probability we have

$$\begin{aligned}
&\mathbf{Adv}^{\mathrm{mPriv}}_{\mathrm{MGM}_{Func(\{0,1\}^n)}}(\mathcal{A}) = \Pr\left[\mathcal{A}^{\mathcal{E}} \Rightarrow 1 \,\cap\, \widetilde{\mathbf{Dom}}^q\ \mathit{coll}\right] + \\
&\quad + \left(\Pr\left[\mathcal{A}^{\mathcal{E}} \Rightarrow 1 \,\cap\, \widetilde{\mathbf{Dom}}^q\ \overline{\mathit{coll}}\right] - \Pr\left[\mathcal{A}^{\$} \Rightarrow 1\right]\right) \leqslant \\
&\quad \leqslant \Pr\left[\widetilde{\mathbf{Dom}}^q\ \mathit{coll}\right] + \left(\Pr\left[\mathcal{A}^{\mathcal{E}} \Rightarrow 1 \,\cap\, \widetilde{\mathbf{Dom}}^q\ \overline{\mathit{coll}}\right] - \Pr\left[\mathcal{A}^{\$} \Rightarrow 1\right]\right).
\end{aligned}$$

Consider the difference $\Pr\left[\mathcal{A}^{\mathcal{E}} \Rightarrow 1 \,\cap\, \widetilde{\mathbf{Dom}}^q\ \overline{\mathit{coll}}\right] - \Pr\left[\mathcal{A}^{\$} \Rightarrow 1\right]$.

Note that the output of the adversary $\mathcal{A}$ is determined by the values $\Gamma^1, T_1, \dots, \Gamma^q, T_q$. By definition,

$$\begin{aligned}
&\Pr\left[\mathcal{A}^{\mathcal{E}} \Rightarrow 1 \,\cap\, \widetilde{\mathbf{Dom}}^q\ \overline{\mathit{coll}}\right] = \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ \mathcal{A}\Rightarrow 1}} \Pr\left[\widetilde{\mathbf{Dom}}^q\ \overline{\mathit{coll}} \cap \left\{\substack{\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j}\right\}_{j=1}^q\right] = \\
&\quad = \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ \mathcal{A}\Rightarrow 1}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ \mathbf{Dom}^q\ \overline{\mathit{coll}}}} \Pr\left[\left\{\substack{\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j}\right\}_{j=1}^q \cap \left\{\substack{\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j}\right\}_{j=1}^q\right] = \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ \mathcal{A}\Rightarrow 1}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ \mathbf{Dom}^q\ \overline{\mathit{coll}}}} \frac{1}{2^{n(2\sigma+2q)+sq}} \leqslant \\
&\quad \leqslant \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ \mathcal{A}\Rightarrow 1}} \#\left\{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q}\right\} \cdot \frac{1}{2^{n(2\sigma+2q)+sq}} = \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ \mathcal{A}\Rightarrow 1}} \frac{1}{2^{n\sigma+sq}}.
\end{aligned}$$

Similarly,

$$\Pr\left[\mathcal{A}^{\$} \Rightarrow 1\right] = \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ \mathcal{A}\Rightarrow 1}} \Pr\left[\left\{\substack{\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j}\right\}_{j=1}^q\right] = \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ \mathcal{A}\Rightarrow 1}} \frac{1}{2^{n\sigma+sq}}.$$

Therefore, the following inequality holds:

$$\Pr\left[\mathcal{A}^{\mathcal{E}} \Rightarrow 1 \,\cap\, \widetilde{\mathbf{Dom}}^q\ \overline{\mathit{coll}}\right] - \Pr\left[\mathcal{A}^{\$} \Rightarrow 1\right] \leqslant 0.$$

Consequently, we have

$$\mathbf{Adv}^{\text{mPriv}}_{\text{MGM}_{Func(\{0,1\}^n)}}(\mathcal{A}) \leqslant \Pr\left[\widetilde{\mathbf{Dom}}^q \ coll\right].$$

Thus, using Corollary 6.3 and Lemma 6.1 we obtain the desirable bound:

$$\mathbf{Adv}^{\text{mPriv}}_{\text{MGM}_{Perm(\{0,1\}^n)}}(\mathcal{A}) \leqslant \mathbf{Adv}^{\text{mPriv}}_{\text{MGM}_{Func(\{0,1\}^n)}}(\mathcal{A}) + \mathbf{Adv}^{\text{PRF}}_{Perm(\{0,1\}^n)}(\mathcal{A}') \leqslant$$
$$\leqslant \Pr\left[\widetilde{\mathbf{Dom}}^q \ coll\right] + \frac{(2\sigma+3q)^2}{2^{n+1}} \leqslant \frac{\sigma^2+8\sigma q+3q^2}{2^n} + \frac{4\sigma^2+12\sigma q+9q^2}{2^{n+1}} \leqslant \frac{3(\sigma+3q)^2}{2^n}.$$

The second inequality follows from the fact that a PRF-breaking adversary $\mathcal{A}'$ makes at most $q' = 2\sigma + 3q$ queries to simulate the encryption oracle. □

6.2 mAuthenticity-security of MGM mode

The adversary for the mAuthenticity notion is defined by the same functions as for the mPrivacy notion, and by additional functions that defines the adversary's output, a forgery (N, X, T). For the adversary that makes q couples of tied queries to the encryption oracle, the output of these functions depends on $2q$ variables:

$N = N^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^q, T_q): \ \{0,1\}^{n\times *} \times \{0,1\}^s \times \ldots \times \{0,1\}^{n\times *} \times \{0,1\}^s \to \{0,1\}^{n-1}$.

$X = X^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^q, T_q): \ \{0,1\}^{n\times *} \times \{0,1\}^s \times \ldots \times \{0,1\}^{n\times *} \times \{0,1\}^s \to \{0,1\}^{n\times *}$.

$T = T^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^q, T_q): \ \{0,1\}^{n\times *} \times \{0,1\}^s \times \ldots \times \{0,1\}^{n\times *} \times \{0,1\}^s \to \{0,1\}^s$.

These functions satisfy the following requirement (non-trivial forgery):

$$(N, X, T) \notin \left\{(N_i, X^i, T_i)\right\}_{i=1}^q, \ \forall \ \Gamma^1, T_1, \ldots, \Gamma^q, T_q.$$

Lemma 6.5. *For any mAuthenticity-breaking adversary $\mathcal{A}$, that makes at most q couples of tied encryption queries with the total value of X lengths at most σ blocks and outputs a forgery with the X length at most l blocks, the following inequality holds*

$$\mathbf{Adv}^{\text{mAuth}}_{\text{MGM}_{Func(\{0,1\}^n)}}(\mathcal{A}) \leqslant \frac{8ql + 2\sigma(l+4) + 5q + 2l + 2}{2^n} + \Pr\left[\widetilde{\mathbf{Dom}}^q \ coll\right] + \frac{2}{2^s}.$$

Proof. We have

$$\mathbf{Adv}^{\text{mAuth}}_{\text{MGM}_{Func(\{0,1\}^n)}}(\mathcal{A}) = \Pr\left[\mathcal{A}^{\mathcal{E}} \ forges\right] = \Pr\left[\mathcal{A}^{\mathcal{E}} \ forges \cap \widetilde{\mathbf{Dom}}^q \ coll\right] +$$
$$+ \Pr\left[\mathcal{A}^{\mathcal{E}} \ forges \cap \widetilde{\mathbf{Dom}}^q \ \overline{coll}\right] \leqslant \Pr\left[\mathcal{A}^{\mathcal{E}} \ forges \cap \widetilde{\mathbf{Dom}}^q \ coll\right] + \Pr\left[\widetilde{\mathbf{Dom}}^q \ \overline{coll}\right].$$

Note that after fixation of the values $\Gamma^j, T_j, \ j = 1, \ldots, q$

1. the random variables $\widetilde{l}_j$ take the fixed values $l_j = l_j^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{j-1}, T_{j-1})$, $j = 1, \ldots, q$.
2. in the tuple $\widetilde{\mathbf{Dom}}^q$ the random variables $\widetilde{N}_j$ take the fixed values $N_j = N_j^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{j-1}, T_{j-1})$, $j = 1, \ldots, q$.

3. the random variables $\widetilde{X}^j$ take the fixed values $X^j = X_j^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{j-1}, T_{j-1}, \Gamma^j),\ j = 1, \ldots, q.$
4. the random variables $\widetilde{X}$, $\widetilde{N}$, $\widetilde{T}$ take the fixed values $X = X^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^q, T_q)$, $N = N^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^q, T_q)$, $T = T^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^q, T_q)$. Without loss of generality we assume that the length of the tuple X is exactly l blocks. The tuple X with the length less then l can be filled up by all-zero blocks since for such a filling the tag will be the same.

Then,

$$\Pr\left[\mathcal{A}^{\mathcal{E}}\ forges \cap \widetilde{\mathbf{Dom}}^q\ \overline{coll}\right] = \underbrace{\sum_{\substack{\Gamma^1,\ldots,\Gamma^q\\ T_1,\ldots,T_q:\\ N\notin\{N_1,\ldots,N_q\}}} \Pr\left[\mathcal{A}^{\mathcal{E}}\ forges \cap \widetilde{\mathbf{Dom}}^q\ \overline{coll} \cap \left\{\substack{\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j}\right\}_{j=1}^q\right] +}_{sum_1}$$

$$+ \underbrace{\sum_{\substack{\Gamma^1,\ldots,\Gamma^q\\ T_1,\ldots,T_q:\\ N\in\{N_1,\ldots,N_q\}}} \Pr\left[\mathcal{A}^{\mathcal{E}}\ forges \cap \widetilde{\mathbf{Dom}}^q\ \overline{coll} \cap \left\{\substack{\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j}\right\}_{j=1}^q\right]}_{sum_2}.$$

Case 1. Consider the first summand sum_1.

$$sum_1 = \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\notin\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ \mathbf{Dom}^q\ \overline{coll}}} \Pr\left[\mathcal{A}^{\mathcal{E}}\ forges \cap \left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^{q} \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j\end{smallmatrix}\right\}_{j=1}^{q}\right] \leqslant$$

$$\leqslant \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\notin\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ \mathbf{Dom}^q\ \overline{coll}\\ 1\|N\in\mathbf{Dom}^q}} \Pr\left[\left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^{q} \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j\end{smallmatrix}\right\}_{j=1}^{q}\right] +$$

$$+ \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\notin\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ \mathbf{Dom}^q\ \overline{coll}\\ 1\|N\notin\mathbf{Dom}^q}} \Pr\left[\mathcal{A}^{\mathcal{E}}\ forges \cap \left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^{q} \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j\end{smallmatrix}\right\}_{j=1}^{q}\right] \leqslant$$

$$\leqslant \underbrace{\sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\notin\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ \mathbf{Dom}^q\ \overline{coll}\\ 1\|N\in\mathbf{Dom}^q}} \Pr\left[\left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^{q} \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j\end{smallmatrix}\right\}_{j=1}^{q}\right]}_{sum_1^1} +$$

$$+ \underbrace{\sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\notin\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ \mathbf{Dom}^q\ \overline{coll}\\ 1\|N\notin\mathbf{Dom}^q}} \sum_{\substack{Z:\\ Z\cap\mathbf{Dom}^q\neq\emptyset\ \vee\\ 1\|N\in Z}} \Pr\left[\left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^{q} \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j\end{smallmatrix}\right\}_{j=1}^{q} \cap \left\{\widetilde{Z}=Z\right\}\right]}_{sum_1^2} +$$

$$+ \underbrace{\sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\notin\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ \mathbf{Dom}^q\ \overline{coll}\\ 1\|N\notin\mathbf{Dom}^q}} \sum_{\substack{Z:\\ Z\cap\mathbf{Dom}^q=\emptyset\\ 1\|N\notin Z}} \sum_{\substack{H:\\ \tau\in\mathbf{Dom}^q\vee\\ \tau=1\|N\vee\\ \tau\in Z}} \Pr\left[\left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^{q} \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j\end{smallmatrix}\right\}_{j=1}^{q} \cap \left\{\begin{smallmatrix}\widetilde{Z}=Z\\ \widetilde{H}=H\end{smallmatrix}\right\}\right] .+}_{sum_1^3}$$

$$+ \underbrace{\sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\notin\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ \mathbf{Dom}^q\ \overline{coll}\\ 1\|N\notin\mathbf{Dom}^q}} \sum_{\substack{Z:\\ Z\cap\mathbf{Dom}^q=\emptyset\\ 1\|N\notin Z}} \sum_{\substack{H:\\ \tau\notin\mathbf{Dom}^q\\ \tau\neq1\|N\\ \tau\notin Z}} \Pr\left[\mathcal{A}^{\mathcal{E}}\ forges \cap \left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^{q} \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j\end{smallmatrix}\right\}_{j=1}^{q} \cap \left\{\begin{smallmatrix}\widetilde{Z}=Z\\ \widetilde{H}=H\end{smallmatrix}\right\}\right].}_{sum_1^4}$$

Consider the first summand sum_1^1. By the same reasoning as in the proof of Lemma 6.1 (case of estimating cardinality of the set A) we obtain the following estimation:

$$sum_1^1 = \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\notin\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ \mathbf{Dom}^q\ \overline{coll}\\ 1\|N\in\mathbf{Dom}^q}} \frac{1}{2^{n(2\sigma+2q)+sq}} \leqslant \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\notin\{N_1,\dots,N_q\}}} \underbrace{\#\left\{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ 1\|N\in\mathbf{Dom}^q}\right\}}_{=(2\sigma+q)\cdot 2^{n(\sigma+2q-1)}} \cdot \frac{1}{2^{n(2\sigma+2q)+sq}} \leqslant$$

$$\leqslant 2^{n\sigma+sq}\cdot(2\sigma+q)\cdot 2^{n(\sigma+2q-1)}\cdot\frac{1}{2^{n(2\sigma+2q)+sq}} = \frac{(2\sigma+q)}{2^n}.$$

Consider the second summand sum_1^2. By the same reasoning as in the proof of Lemma 6.1 (case of estimating cardinality of the set B) we obtain the following estimation:

$$sum_1^2 = \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\notin\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ \mathbf{Dom}^q\ \overline{coll}\\ 1\|N\notin\mathbf{Dom}^q}} \sum_{\substack{Z:\\ Z\cap\mathbf{Dom}^q\neq\emptyset\ \vee\\ 1\|N\in Z}} \frac{1}{2^{n(2\sigma+2q)+n+sq}} =$$

$$= \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\notin\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ \mathbf{Dom}^q\ \overline{coll}\\ 1\|N\notin\mathbf{Dom}^q}} \underbrace{\#\left\{\substack{Z:\\ Z\cap\mathbf{Dom}^q\neq\emptyset\ \vee\\ 1\|N\in Z}\right\}}_{\leqslant 4ql+\sigma(l+1)-q+l} \cdot \frac{1}{2^{n(2\sigma+2q)+n+sq}} \leqslant$$

$$\leqslant 2^{n\sigma+sq}\cdot 2^{n(\sigma+2q)}\cdot(4ql+\sigma(l+1)-q+l)\cdot\frac{1}{2^{n(2\sigma+2q)+n+sq}} = \frac{4ql+\sigma(l+1)-q+l}{2^n}.$$

Consider the third summand sum_1^3. By the same reasoning as in the proof of Lemma 6.1 (case of estimating cardinality of the set C) we obtain the following estimation:

$$sum_1^3 = \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\notin\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ \mathbf{Dom}^q\ \overline{coll}\\ 1\|N\notin\mathbf{Dom}^q}} \sum_{\substack{Z:\\ Z\cap\mathbf{Dom}^q=\emptyset\\ 1\|N\notin Z}} \sum_{\substack{H:\\ \tau\in\mathbf{Dom}^q\vee\\ \tau=1\|N\vee\\ \tau\in Z}} \Pr\left[\left\{\substack{\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j}\right\}_{j=1}^q \cap \left\{\substack{\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j}\right\}_{j=1}^q \cap \left\{\substack{\widetilde{Z}=Z\\ \widetilde{H}=H}\right\}\right] =$$

$$= \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\notin\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ \mathbf{Dom}^q\ \overline{coll}\\ 1\|N\notin\mathbf{Dom}^q}} \sum_{\substack{Z:\\ Z\cap\mathbf{Dom}^q=\emptyset\\ 1\|N\notin Z}} \underbrace{\#\left\{\substack{H:\\ \tau\in\mathbf{Dom}^q\vee\\ \tau=1\|N\vee\\ \tau\in Z}\right\}}_{\leqslant(2\sigma+3q+l+1)\cdot 2^{nl-n}} \cdot \frac{1}{2^{n(2\sigma+2q)+n(l+1)+sq}} \leqslant$$

$$\leqslant 2^{n\sigma+sq}\cdot 2^{n(\sigma+2q)}\cdot 2^n\cdot(2\sigma+3q+l+1)\cdot 2^{nl-n}\cdot\frac{1}{2^{n(2\sigma+2q)+n(l+1)+sq}} = \frac{2\sigma+3q+l+1}{2^n}.$$

Consider the forth summand sum_1^4. We have:

$$sum_1^4 = \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\notin\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ \mathbf{Dom}^q\ \overline{coll}\\ 1\|N\notin\mathbf{Dom}^q}} \sum_{\substack{Z:\\ Z\cap\mathbf{Dom}^q=\emptyset\\ 1\|N\notin Z}} \sum_{\substack{H:\\ \tau\notin\mathbf{Dom}^q\\ \tau\neq 1\|N\\ \tau\notin Z}} \Pr\left[\left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^q \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j\end{smallmatrix}\right\}_{j=1}^q \cap \left\{\begin{smallmatrix}\widetilde{Z}=Z\\ \widetilde{H}=H\\ \mathrm{msb}_s(\rho(\tau))=T\end{smallmatrix}\right\}\right] =$$

$$= \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\notin\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,Z^q\\ H^1,\dots,H^q:\\ \mathbf{Dom}^q\ \overline{coll}\\ 1\|N\notin\mathbf{Dom}^q}} \sum_{\substack{Z:\\ Z\cap\mathbf{Dom}^q=\emptyset\\ 1\|N\notin Z}} \sum_{\substack{H:\\ \tau\notin\mathbf{Dom}^q\\ \tau\neq 1\|N\\ \tau\notin Z}} \frac{1}{2^{n(2\sigma+2q)+n(l+1)+sq+s}} \leqslant$$

$$\leqslant 2^{n\sigma+sq}\cdot 2^{n(\sigma+2q)}\cdot 2^n\cdot 2^{nl}\cdot\frac{1}{2^{n(2\sigma+2q)+n(l+1)+sq+s}} = \frac{1}{2^s}.$$

Thus,

$$sum_1 \leqslant \frac{2\sigma+q}{2^n} + \frac{4ql+\sigma(l+1)-q+l}{2^n} + \frac{2\sigma+3q+l+1}{2^n} + \frac{1}{2^s} =$$

$$= \frac{4ql+\sigma(l+5)+3q+2l+1}{2^n} + \frac{1}{2^s}.$$

Case 2. Consider the summand sum_2.

Note that after additional fixation of the values H^j, $j=1,\dots,q$, in the tuple $\widetilde{\mathbf{Dom}}^q$ the random variables $\widetilde{\tau}_j$ take the fixed values $\tau_j = \sum_{k_j=1}^{l_j} H^j_{k_j}\cdot X^j_{k_j}$, $j=1,\dots,q$.

Suppose $N=N_u$ for some u, $1\leqslant u\leqslant q$. We will consider only the case $l_u<l$ since in this case new $l-l_u$ blocks Z^u_k appear and these blocks may collide with values from $\mathbf{Dom}^q$. By Z_{add} we denote the tuple $(Z^u_{l_u+1},\dots,Z^u_l)$, by $\hat{Z}^u$ — the tuple $Z^u\|Z_{add}$, and by $\widehat{\mathbf{Dom}}^q$ — the tuple $\mathbf{Dom}^q\|Z_{add}$.

Note that after additional fixation of the values H^u_k, $k=(l_u+1),\dots,l$, the random variable $\widetilde{\tau}$ takes the fixed value $\tau=\sum_{k=1}^{l} H^u_k\cdot X_k$, $j=1,\dots,q$. Denote by $\hat{H}^u$ the set consisting of l_u blocks of H^u and $l-l_u$ blocks $H^u_k=\rho(Z^u_k)$, $k=(l_u+1),\dots,l$.

Thus,

$$sum_2 = \sum_{\substack{\Gamma^1,\ldots,\Gamma^q\\ T_1,\ldots,T_q:\\ N\in\{N_1,\ldots,N_q\}}} \Pr\left[\mathcal{A}^{\mathcal{E}}\ forges \cap \widetilde{\mathbf{Dom}}^q\ \overline{coll} \cap \left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^q\right] \leqslant$$

$$\leqslant \underbrace{\sum_{\substack{\Gamma^1,\ldots,\Gamma^q\\ T_1,\ldots,T_q:\\ N\in\{N_1,\ldots,N_q\}}} \sum_{\substack{Y^1,\ldots,Y^q\\ Z^1,\ldots,\hat{Z}^u,\ldots,Z^q\\ H^1,\ldots,H^q:\\ \mathbf{Dom}^q\ \overline{coll}\\ Z_{add}\cap\mathbf{Dom}^q\neq\emptyset}} \Pr\left[\left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^q \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j,\ j\neq u\\ \widetilde{H}^j=H^j\end{smallmatrix}\right\}_{j=1}^q \cap \left\{\widetilde{\hat{Z}}^u=\hat{Z}^u\right\}\right]+}_{sum_2^1}$$

$$+\underbrace{\sum_{\substack{\Gamma^1,\ldots,\Gamma^q\\ T_1,\ldots,T_q:\\ N\in\{N_1,\ldots,N_q\}}} \sum_{\substack{Y^1,\ldots,Y^q\\ Z^1,\ldots,\hat{Z}^u,\ldots,Z^q\\ H^1,\ldots,\hat{H}^u,\ldots,H^q:\\ \widehat{\mathbf{Dom}}^q\ \overline{coll}\\ \tau\in\widehat{\mathbf{Dom}}^q}} \Pr\left[\left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^q \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j,\ j\neq u\\ \widetilde{H}^j=H^j,\ j\neq u\end{smallmatrix}\right\}_{j=1}^q \cap \left\{\begin{smallmatrix}\widetilde{\hat{Z}}^u=\hat{Z}^u\\ \widetilde{\hat{H}}^u=\hat{H}^u\end{smallmatrix}\right\}\right]+}_{sum_2^2}$$

$$+\underbrace{\sum_{\substack{\Gamma^1,\ldots,\Gamma^q\\ T_1,\ldots,T_q:\\ N\in\{N_1,\ldots,N_q\}}} \sum_{\substack{Y^1,\ldots,Y^q\\ Z^1,\ldots,\hat{Z}^u,\ldots,Z^q\\ H^1,\ldots,\hat{H}^u,\ldots,H^q:\\ \widehat{\mathbf{Dom}}^q\ \overline{coll}\\ \tau\notin\widehat{\mathbf{Dom}}^q}} \Pr\left[\mathcal{A}^{\mathcal{E}}\ forges \cap \left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^q \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j,\ j\neq u\\ \widetilde{H}^j=H^j,\ j\neq u\end{smallmatrix}\right\}_{j=1}^q \cap \left\{\begin{smallmatrix}\widetilde{\hat{Z}}^u=\hat{Z}^u\\ \widetilde{\hat{H}}^u=\hat{H}^u\end{smallmatrix}\right\}\right].}_{sum_2^3}$$

Consider the first summand sum_2^1.

$$sum_2^1 = \sum_{\substack{\Gamma^1,\ldots,\Gamma^q\\ T_1,\ldots,T_q:\\ N\in\{N_1,\ldots,N_q\}}} \sum_{\substack{Y^1,\ldots,Y^q\\ Z^1,\ldots,\hat{Z}^u,\ldots,Z^q\\ H^1,\ldots,H^q:\\ \mathbf{Dom}^q\ \overline{coll}\\ Z_{add}\cap\mathbf{Dom}^q\neq\emptyset}} \frac{2^{n(2^n-(2\sigma+3q))}\cdot 2^{(n-s)q}}{2^{n2^n}} \leqslant$$

$$\leqslant \sum_{\substack{\Gamma^1,\ldots,\Gamma^q\\ T_1,\ldots,T_q:\\ N\in\{N_1,\ldots,N_q\}}} \sum_{\substack{Y^1,\ldots,Y^q\\ Z^1,\ldots,Z^{u-1},\\ Z^{u+1},\ldots,Z^q\\ H^1,\ldots,H^q}} \sum_{\substack{\hat{Z}^u:\\ Z_{add}\cap\mathbf{Dom}^q\neq\emptyset}} \frac{1}{2^{n(2\sigma+2q)+sq}} \leqslant$$

$$\leqslant \sum_{\substack{\Gamma^1,\ldots,\Gamma^q\\ T_1,\ldots,T_q:\\ N\in\{N_1,\ldots,N_q\}}} \sum_{\substack{Y^1,\ldots,Y^q\\ Z^1,\ldots,Z^{u-1},\\ Z^{u+1},\ldots,Z^q\\ H^1,\ldots,H^q}} \underbrace{\#\left\{\begin{smallmatrix}\hat{Z}^u:\\ Z_{add}\cap\mathbf{Dom}^q\neq\emptyset\end{smallmatrix}\right\}}_{D}\cdot\frac{1}{2^{n(2\sigma+2q)+sq}}.$$

Estimate the cardinality of the set D.

$$D \subset \bigcup_{j\in\{1,\dots,q\}\setminus\{u\}} \left\{ \substack{\hat{Z}^u: \\ Z_{add}\cap Z^j \neq \emptyset} \right\} \cup \bigcup_{j=1}^{q} \left\{ \substack{\hat{Z}^u: \\ \tau_j \in Z_{add}} \right\} \cup \bigcup_{j=1}^{q} \bigcup_{k_j=1}^{l_j} \left\{ \substack{\hat{Z}^u: \\ Y^j_{k_j} \in Z_{add}} \right\} \cup \bigcup_{j=1}^{q} \bigcup_{b\in\{0,1\}} \left\{ \substack{\hat{Z}^u: \\ b\|N_j \in Z_{add}} \right\}.$$

Thus, the cardinality of the set D can be estimated in the following way:

$$\begin{aligned} \#D \leqslant \sum_{j\in\{1,\dots,q\}\setminus\{u\}} \underbrace{\# \left\{ \substack{\hat{Z}^u: \\ Z_{add}\cap Z^j \neq \emptyset} \right\}}_{=l_j+(l-l_u)-1} + \sum_{j=1}^{q} \underbrace{\# \left\{ \substack{\hat{Z}^u: \\ \tau_j \in Z_{add}} \right\}}_{=l-l_u} + \\ + \sum_{j=1}^{q} \sum_{k_j=1}^{l_j} \underbrace{\# \left\{ \substack{\hat{Z}^u: \\ Y^j_{k_j} \in Z_{add}} \right\}}_{=l-l_u} + \sum_{j=1}^{q} \sum_{b\in\{0,1\}} \underbrace{\# \left\{ \substack{\hat{Z}^u: \\ b\|N_j \in Z_{add}} \right\}}_{l-l_u} = \\ = (\sigma - l_u) + (q-1)(l-l_u) - (q-1) + q(l-l_u) + \sigma(l-l_u) + 2q(l-l_u) = \\ = 4q(l-l_u) + \sigma(l-l_u) + \sigma - l_u - q + 1 - l + l_u \leqslant 4ql + \sigma(l+1) - q + 1 - l. \end{aligned}$$

Thus,

$$\begin{aligned} sum_2^1 \leqslant \sum_{\substack{\Gamma^1,\dots,\Gamma^q \\ T_1,\dots,T_q: \\ N\in\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q \\ Z^1,\dots,Z^{u-1}, \\ Z^{u+1},\dots,Z^q \\ H^1,\dots,H^q}} (4ql + \sigma(l+1) - q + 1 - l) \cdot \frac{1}{2^{n(2\sigma+2q)+sq}} \leqslant \\ \leqslant 2^{n\sigma+sq} \cdot 2^{n(\sigma+2q)-n} \cdot \frac{(4ql + \sigma(l+1) - q + 1 - l)}{2^{n(2\sigma+2q)+sq}} = \frac{4ql + \sigma(l+1) - q + 1 - l}{2^n}. \end{aligned}$$

Remark 6.2. Note that the other cases $l_u = l$ and $l_u > l$ are covered by the case $l_u < l$, since for these cases the set Z_{add} is empty and $sum_2^1 = 0$.

Consider the second summand sum_2^2.

$$sum_2^2 = \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\in\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,\hat{Z}^u,\dots,Z^q\\ H^1,\dots,\hat{H}^u,\dots,H^q:\\ \widehat{\mathbf{Dom}}^q\ \overline{coll}\\ \tau\in\widehat{\mathbf{Dom}}^q}} \Pr\left[\left\{\substack{\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j}\right\}_{j=1}^{q} \cap \left\{\substack{\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j,\ j\neq u\\ \widetilde{H}^j=H^j,\ j\neq u}\right\}_{j=1}^{q} \cap \left\{\substack{\widetilde{\hat{Z}^u}=\hat{Z}^u\\ \widetilde{\hat{H}^u}=\hat{H}^u}\right\}\right] =$$

$$= \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\in\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,\hat{Z}^u,\dots,Z^q\\ H^1,\dots,\hat{H}^u,\dots,H^q:\\ \widehat{\mathbf{Dom}}^q\ \overline{coll}\\ \tau\in\widehat{\mathbf{Dom}}^q}} \frac{\#\left\{\rho:\ \substack{\rho(0\|N_j)=Y_1^j\\ \rho(1\|N_j)=Z_1^j\\ \mathrm{msb}_s(\rho(\tau_j))=T_j},\ \substack{\rho(Y_{k_j}^j)=\Gamma_{k_j}^j\\ \rho(Z_{k_j}^j)=H_{k_j}^j},\ \rho(Z_k^u)=H_k^u,\ \substack{j=\overline{1,q}\\ k_j=\overline{1,l_j}\\ k=\overline{l_u+1,l}}\right\}}{2^{n2^n}} =$$

$$= \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\in\{N_1,\dots,N_q\}}} \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,\hat{Z}^u,\dots,Z^q\\ H^1,\dots,\hat{H}^u,\dots,H^q:\\ \widehat{\mathbf{Dom}}^q\ \overline{coll}\\ \tau\in\widehat{\mathbf{Dom}}^q}} \frac{2^{n(2^n-(2\sigma+3q)-(l-l_u))}\cdot 2^{(n-s)q}}{2^{n2^n}} \leqslant$$

$$\leqslant \sum_{\substack{\Gamma^1,\dots,\Gamma^q\\ T_1,\dots,T_q:\\ N\in\{N_1,\dots,N_q\}}} \underbrace{\#\left\{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,\hat{Z}^u,\dots,Z^q\\ H^1,\dots,\hat{H}^u,\dots,H^q:\\ \tau\in\widehat{\mathbf{Dom}}^q}\right\}}_{E}\cdot\frac{1}{2^{n(2\sigma+2q)+n(l-l_u)+sq}}.$$

Estimate the cardinality of the set E for the fixed values Γ^j, T_j, $j=1,\dots,q$ (consequently, for the fixed values N_j). Denote by $\hat{X}^u\in\{0,1\}^{n\times l}$ the tuple $(X_1^u,\dots,X_{l_u}^u,0^n,\dots,0^n)$. The set E can be covered by the union of the following sets:

$$E\subset \bigcup_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,\hat{Z}^u,\dots,Z^q\\ H^1,\dots,H^{u-1},\\ H^{u+1},\dots,H^q}} \left(\left\{\substack{\hat{H}^u:\\ \tau\in\widehat{\mathbf{Dom}}^q\setminus\{\widetilde{\tau}_u\}}\right\}\cup\left\{\substack{\hat{H}^u:\\ \tau=\tau_u}\right\}\right) = \bigcup_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,\hat{Z}^u,\dots,Z^q\\ H^1,\dots,H^{u-1},\\ H^{u+1},\dots,H^q}} \left(\left\{\substack{\hat{H}^u:\\ \tau\in\widehat{\mathbf{Dom}}^q\setminus\{\widetilde{\tau}_u\}}\right\}\cup\left\{\substack{\hat{H}^u:\\ \sum_{k=1}^l H_k^u(X_k-\hat{X}_k^u)=0}\right\}\right).$$

Thus, the cardinality of the set E can be estimated in the following way:

$$\#E\leqslant \sum_{\substack{Y^1,\dots,Y^q\\ Z^1,\dots,\hat{Z}^u,\dots,Z^q\\ H^1,\dots,H^{u-1},\\ H^{u+1},\dots,H^q}} \left(\underbrace{\#\left\{\substack{\hat{H}^u:\\ \tau\in\widehat{\mathbf{Dom}}^q\setminus\{\widetilde{\tau}_u\}}\right\}}_{\leqslant(|\widehat{\mathbf{Dom}}^q|-1)\cdot 2^{nl-n}} + \underbrace{\#\left\{\substack{\hat{H}^u:\\ \sum_{k=1}^l H_k^u(X_k-\hat{X}_k^u)=0}\right\}}_{=2^{nl-n}}\right) =$$

$$= 2^{n(\sigma+2q-l_u)}\cdot(2\sigma+3q+l-l_u)\cdot 2^{nl_u+n(l-l_u)-n}\leqslant(2\sigma+3q+l)\cdot 2^{n(\sigma+2q)+n(l-l_u)-n},$$

$$\forall\ \Gamma^j, T_j, j=1,\dots,q.$$

Thus,

$$sum_2^2 \leqslant \sum_{\substack{\Gamma^1,\ldots,\Gamma^q \\ T_1,\ldots,T_q \\ N\in\{N_1,\ldots,N_q\}}} \frac{(2\sigma+3q+l)\cdot 2^{n(\sigma+2q+l)+n(l-l_u)-n}}{2^{n(2\sigma+2q+l)+n(l-l_u)+sq}} \leqslant \#\left\{\begin{smallmatrix}\Gamma^1,\ldots,\Gamma^q \\ T_1,\ldots,T_q\end{smallmatrix}\right\} \cdot \frac{2\sigma+3q+l}{2^{n\sigma+n+sq}} =$$

$$= 2^{n\sigma+sq}\cdot\frac{2\sigma+3q+l}{2^{n\sigma+n+sq}} = \frac{2\sigma+3q+l}{2^n}.$$

Consider the third summand sum_2^3.

$$sum_2^3 = \sum_{\substack{\Gamma^1,\ldots,\Gamma^q \\ T_1,\ldots,T_q: \\ N\in\{N_1,\ldots,N_q\}}} \sum_{\substack{Y^1,\ldots,Y^q \\ Z^1,\ldots,\hat{Z}^u,\ldots,Z^q \\ H^1,\ldots,\hat{H}^u,\ldots,H^q: \\ \widehat{\mathbf{Dom}}^q\ \overline{coll} \\ \tau\notin\widehat{\mathbf{Dom}}^q}} \Pr\left[\left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j \\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^{q} \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j \\ \widetilde{Z}^j=Z^j,\ j\neq u \\ \widetilde{H}^j=H^j,\ j\neq u\end{smallmatrix}\right\}_{j=1}^{q} \cap \left\{\begin{smallmatrix}\widetilde{\hat{Z}}^u=\hat{Z}^u \\ \widetilde{\hat{H}}^u=\hat{H}^u \\ \mathrm{msb}_s(\rho(\tau))=T\end{smallmatrix}\right\}\right] =$$

$$= \sum_{\substack{\Gamma^1,\ldots,\Gamma^q \\ T_1,\ldots,T_q: \\ N\in\{N_1,\ldots,N_q\}}} \sum_{\substack{Y^1,\ldots,Y^q \\ Z^1,\ldots,\hat{Z}^u,\ldots,Z^q \\ H^1,\ldots,\hat{H}^u,\ldots,H^q: \\ \widehat{\mathbf{Dom}}^q\ \overline{coll} \\ \tau\notin\widehat{\mathbf{Dom}}^q}} \frac{1}{2^{n(2\sigma+2q)+n(l-l_u)+sq+s}} \leqslant$$

$$\leqslant 2^{n\sigma+sq}\cdot 2^{n(\sigma+2q+(l-l_u))}\cdot\frac{1}{2^{n(2\sigma+2q)+n(l-l_u)+sq+s}} = \frac{1}{2^s}.$$

Thus,

$$sum_2 \leqslant \frac{4ql+\sigma(l+1)-q+1-l}{2^n} + \frac{2\sigma+3q+l}{2^n} + \frac{1}{2^s} = \frac{4ql+\sigma(l+3)+2q+1}{2^n} + \frac{1}{2^s}.$$

Finally, the desirable bound is:

$$\mathbf{Adv}^{\mathrm{mAuth}}_{\mathrm{MGM}_{Func(\{0,1\}^n)}}(\mathcal{A}) \leqslant sum_1 + sum_2 + \Pr\left[\widetilde{\mathbf{Dom}}^q\ coll\right] \leqslant$$

$$\leqslant \frac{8ql+2\sigma(l+4)+5q+2l+2}{2^n} + \Pr\left[\widetilde{\mathbf{Dom}}^q\ coll\right] + \frac{2}{2^s}.$$

□

Theorem 6.6. *For any adversary $\mathcal{A}$, that makes at most q couples of tied encryption queries with the total value of X lengths at most σ blocks and outputs a forgery with the X length at most l blocks, the following inequality holds:*

$$\mathbf{Adv}^{\mathrm{mAuth}}_{\mathrm{MGM}_{Perm(\{0,1\}^n)}}(\mathcal{A}) \leqslant \frac{3(\sigma+3q+l+2)^2}{2^n} + \frac{2}{2^s}.$$

Proof. Construct an adversary $\mathcal{A}'$ that breaks PRF-security of the cipher $Perm(\{0,1\}^n)$ using the adversary $\mathcal{A}$. The $\mathcal{A}'$ is constructed as follows. The adversary $\mathcal{A}'$ starts the adversary

$\mathcal{A}$, intercepts $\mathcal{A}$'s queries and processes them by itself. During queries processing the adversary «simulates» the encryption oracle $\mathcal{E}$: implements the oracle functionality according to the definition of the mAuthenticity notion, making the appropriate queries to its own oracle (random permutation π or random function ρ) for each block processing. Note that if the adversary $\mathcal{A}'$ interacts with the oracle π, then it simulates for $\mathcal{A}$ the encryption oracle $\mathcal{E}$ for the $\mathrm{MGM}_{Perm(\{0,1\}^n)}$ mode, and if it interacts with the oracle ρ, then it implements the encryption oracle $\mathcal{E}$ for the $\mathrm{MGM}_{Func(\{0,1\}^n)}$ mode. At the end of $\mathcal{A}$'s work the adversary $\mathcal{A}'$ receives a forgery (N, X, T) and checks the validity of this forgery according to the mAuthenticity notion, making the appropriate queries to its own oracle for blocks processing. As a result the adversary $\mathcal{A}'$ returns 1 if the forgery is valid and returns 0, otherwise. For such an adversary:

$$\begin{aligned}
&\mathbf{Adv}^{\mathrm{PRF}}_{Perm(\{0,1\}^n)}(\mathcal{A}') = \\
&\quad = \Pr\left[\pi \xleftarrow{\mathcal{U}} Perm(\{0,1\}^n) : (\mathcal{A}')^{\pi} \Rightarrow 1\right] - \Pr\left[\rho \xleftarrow{\mathcal{U}} Func(\{0,1\}^n) : (\mathcal{A}')^{\rho} \Rightarrow 1\right] = \\
&\quad = \Pr\left[\pi \xleftarrow{\mathcal{U}} Perm(\{0,1\}^n) : \mathcal{A}^{\mathcal{E}}\ forges\right] - \Pr\left[\rho \xleftarrow{\mathcal{U}} Func(\{0,1\}^n) : \mathcal{A}^{\mathcal{E}}\ forges\right] = \\
&\quad\quad = \mathbf{Adv}^{\mathrm{mAuth}}_{\mathrm{MGM}_{Perm(\{0,1\}^n)}}(\mathcal{A}) - \mathbf{Adv}^{\mathrm{mAuth}}_{\mathrm{MGM}_{Func(\{0,1\}^n)}}(\mathcal{A}).
\end{aligned}$$

Using Corollary 6.3, Lemma 6.5 we obtain the desirable bound:

$$\begin{aligned}
&\mathbf{Adv}^{\mathrm{mAuth}}_{\mathrm{MGM}_{Perm(\{0,1\}^n)}}(\mathcal{A}) \leqslant \mathbf{Adv}^{\mathrm{mAuth}}_{\mathrm{MGM}_{Func(\{0,1\}^n)}}(\mathcal{A}) + \mathbf{Adv}^{\mathrm{PRF}}_{Perm(\{0,1\}^n)}(\mathcal{A}') \leqslant \\
&\quad \leqslant \frac{8ql + 2\sigma(l+4) + 5q + 2l + 2}{2^n} + \frac{2}{2^s} + \Pr\left[\widetilde{\mathbf{Dom}}^{q}\ coll\right] + \frac{(2\sigma + 3q + l + 2)^2}{2^{n+1}} \leqslant \\
&\quad \leqslant \frac{8ql + 2\sigma l + 8\sigma + 5q + 2l + 2}{2^n} + \frac{2}{2^s} + \frac{\sigma^2 + 8\sigma q + 3q^2}{2^n} + \\
&\quad + \frac{3ql + 2\sigma l + 4\sigma + 6q}{2^n} + \frac{(2\sigma + 3q)^2 + (l+2)^2}{2^{n+1}} \leqslant \\
&\quad \leqslant \frac{11ql + 4\sigma l + 12\sigma + 11q}{2^n} + \frac{3\sigma^2 + 14\sigma q + 8q^2 + l^2 + 4l + 4}{2^n} + \frac{2}{2^s} \leqslant \\
&\quad \leqslant \frac{3(\sigma + 3q + l + 2)^2}{2^n} + \frac{2}{2^s}.
\end{aligned}$$

The second inequality is due to that a PRF-breaking adversary $\mathcal{A}'$ for the $Perm(\{0,1\}^n)$ makes at most $2\sigma + 3q$ queries to simulate the encryption oracle and at most $l + 2$ queries to process the last forgery query. □

6.3 Security bounds

Theorem 6.7. *For any Privacy-breaking adversary $\mathcal{A}$, that makes at most q queries with the total length of plaintexts and associated data at most σ blocks, the following inequality holds:*

$$\mathbf{Adv}^{\mathrm{Priv}}_{\mathrm{MGM}_{Perm(\{0,1\}^n)}}(\mathcal{A}) \leqslant \frac{3(\sigma + 4q)^2}{2^n}.$$

Proof. The proof of the theorem follows from Theorem 6.4 and Proposition 5.1. □

Theorem 6.8. *For any Authenticity-breaking adversary $\mathcal{A}$, that makes at most q encryption queries with the total length of plaintexts and associated data at most σ blocks and outputs a forgery with the summary length of ciphertext and associated data at most l blocks, the following inequality holds:*

$$\mathbf{Adv}^{\mathrm{Auth}}_{\mathrm{MGM}_{Perm(\{0,1\}^n)}}(\mathcal{A}) \leqslant \frac{3(\sigma+4q+l+3)^2}{2^n} + \frac{2}{2^s}.$$

Proof. The proof of the theorem follows from Theorem 6.6 and Proposition 5.2. □

Bound comparison. Compare the lower bounds for Authenticity of the GCM mode supposed to be used in TLS 1.3 and the MGM mode considered in the current paper.

The best bound for Authenticity of GCM can be found in [5]:

$$\frac{l+1}{2^s} \cdot \delta_n(\sigma+q+2),$$

where l is the maximal summary block-length of plaintext and associated data, σ is the total block-length of plaintexts, q is the number of messages, n is the block bit-size, s is the tag bit-size, and

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

Assuming that $\sigma+q+2 \leqslant 2^{64}$, we have that $1 \leqslant \delta_n(\sigma+q+2) \leqslant 2$ for $n = 128$, and we get an upper bound

$$\frac{2(l+1)}{2^s}.$$

The specification of TLS 1.3 [12] recommends to encrypt at most 2^{24} full-size records ($l = 2^{12}$ blocks). For $n = 128$ and $s = 64$ we obtain the following upper bounds for probabilities of breaking integrity: $\approx 2^{-51}$ for GCM and $\approx 2^{-54}$ for MGM.

7 Conclusion

In the current paper we provide the lower security (upper insecurity) bounds in the Privacy and Authenticity notions for the new MGM mode which is currently considered as a contender for the standard AEAD mode in Russia. The obtained bounds show that the privacy and authenticity of this mode is provably guaranteed (under security of the used block cipher) up to the birthday paradox bound.

The aim of our future work is the analysis of the mode for an INT-CTXT notions where an adversary has a capability to make several forgery queries.

We thank Igor B. Oshkin for useful discussions and comments during this work.

References

[1] M. Bellare and P. Rogaway, “Introduction to modern cryptography, chapter 4: Symmetric Encryption”, 2004, http://www-cse.ucsd.edu/users/mihir/cse207.

[2] E. Biham and A. Shamir, “Differential Cryptanalysis of DES-like Cryptosystems”, Advances in Cryptology — CRYPTO 1990, Lecture Notes in Computer Science, **537**, ed. A. Menezes, S. Vanstone, Springer, Berlin, Heidelberg, 1991, 2–21.

[3] 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.

[4] N. Ferguson, “Authentication weaknesses in GCM”, May 2005, https://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/CWC-GCM/Ferguson2.pdf.

[5] T. Iwata, K. Ohashi, K. Minematsu, “Breaking and Repairing GCM Security Proofs”, CRYPTO 2012, Lecture Notes in Computer Science, **7417**, Springer, Berlin, Heidelberg, 2012, 31–49.

[6] A. Joux, “Authentication Failures in NIST version of GCM”, 2006, http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/800-38Series-Drafts/GCM/Jouxcomments.pdf.

[7] M.-J. O. Saarinen, “Cycling Attacks on GCM, GHASH and Other Polynomial MACs and Hashes”, Fast Software Encryption (FSE 2012), Lecture Notes in Computer Science, 2012.

[8] M. Matsui, “Linear Cryptanalysis Method for DES Cipher”, Advances in Cryptology — EUROCRYPT 1993, Lecture Notes in Computer Science, **765**, ed. T. Helleseth, Springer, Berlin, Heidelberg, 1994, 402–415.

[9] V. Nozdrunov and V. Shishkin, “Multilinear Galois Mode (MGM)”, *CFRG Draft*, ed. S. Smyshlyaev, 2018, https://datatracker.ietf.org/doc/draft-smyshlyaev-mgm.

[10] V. Nozdrunov, “Parallel and double block cipher mode of operation (PD-mode) for authenticated encryption”, CTCrypt 2017, 2017, 36–45.

[11] C. Ramsay and J. Lohuis, “TEMPEST attacks against AES. Covertly stealing keys for 200 euro”, 2017.

[12] E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3”, Internet Standards Track document, Internet Engineering Task Force (IETF), August 2018, https://tools.ietf.org/html/rfc8446.

[13] P. Rogaway, “Nonce-Based Symmetric Encryption”, Fast Software Encryption (FSE 2004), Lecture Notes in Computer Science, **3017**, ed. B. Roy and W. Meier, Springer, Berlin, Heidelberg, 2004, 348–358.

[14] T. Shrimpton, “A Characterization of Authenticated-Encryption as a Form of Chosen-Ciphertext Security”, *IACR ePrint Archive*, 2004, Report 2004/272, https://eprint.iacr.org/2004/272.