Toward a Fully Secure Authenticated Encryption Scheme From a Pseudorandom Permutation

Wonseok Choi, Byeonghak Lee, Jooyoung Lee*, and Yeongmin Lee

KAIST, Daejeon, Korea
{krwioh,lbh0307,dudals4780,hicalf}@kaist.ac.kr

Abstract. In this paper, we propose a new block cipher-based authenticated encryption scheme, dubbed the Synthetic Counter with Masking (SCM) mode. SCM follows the NSIV paradigm proposed by Peyrin and Seurin (CRYPTO 2016), where a keyed hash function accepts a nonce N with associated data and a message, yielding an authentication tag T, and then the message is encrypted by a counter-like mode using both T and N. Here we move one step further by *encrypting nonces*; in the encryption part, the inputs to the block cipher are determined by T, counters, and an encrypted nonce, and all its outputs are also masked by an (additional) encrypted nonce, yielding keystream blocks.
As a result, we obtain, for the first time, a block cipher-based authenticated encryption scheme of rate 1/2 that provides n-bit security with respect to the query complexity (ignoring the influence of message length) in the nonce-respecting setting, and at the same time guarantees graceful security degradation in the faulty nonce model, when the underlying n-bit block cipher is modeled as a secure pseudorandom permutation. Seen as a slight variant of GCM-SIV, SCM is also parallelizable and inverse-free, and its performance is still comparable to GCM-SIV.

Keywords: authenticated encryption, beyond-birthday-bound security, nonce-misuse resistance, graceful degradation, block cipher

1 Introduction

Authenticated Encryption. Authenticated encryption (AE) aims at achieving the two fundamental security goals of symmetric key cryptography, namely, the confidentiality and the authenticity of data. With a significant amount of research in this area, we now have a rich set of general-purpose AE schemes, some already standardized (e.g., GCM [20] and CCM [26]) and some expected to be adopted by new applications and standards (e.g., the CAESAR finalists COLM [1], Ascon [7], Deoxys II [17], OCB [19], ACORN [27], and AEGIS-128 [28]).

* This work was supported by Institute for Information & communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT) (No.2019-0-01343, Regional strategic industry convergence security core talent training business)

Such AE schemes are built on top of various cryptographic primitives such as permutations and (tweakable) block ciphers. Most of recent constructions accept associated data (AD), which are authenticated but not encrypted. In this paper, we will also consider AE schemes with associated data.

Nonce-Misuse Resistance. Nonces or initial vectors (IVs) are used in most encryption schemes in order to guarantee the variability of the ciphertext. In particular, nonces will guarantee stronger security in the authentication part than deterministic constructions when they are never reused. On the other hand, only a single nonce repetition can completely break the security of the scheme. For example, GCM leaks its hash key as soon as a a single nonce is used twice. However, it might be challenging to maintain the uniqueness of the nonce in certain environments, for example, in a stateless device where good quality randomness is not available. A faulty implementation of the AE scheme might also repeat nonces. For this reason, there has been a considerable amount of research on the design of AE schemes achieving nonce-misuse resistance.

Rogaway and Shrimpton [25] formalized the notion of misuse-resistant AE (MRAE) and proposed a method of turning a deterministic AE scheme into a nonce-based MRAE scheme. In this way, nonce repetitions do not affect the overall security of the scheme as long as a triple of nonce, AD and message values is not repeated. MRAE schemes include EAX [2], SIV [25], AEZ [11], and GCM-SIV [10]. Later, this notion has been refined by viewing the adversarial distinguishing advantage as a function of the maximum number of multicollisions in nonce values (amongst all encryption queries) [24]. Recently, Dutta et. al. [8] introduced the *faulty nonce model*; an adversarial query is called a *faulty query* if there exists a previous query with the same nonce. Here, the adversarial distinguishing advantage is analyzed as a function of the number of faulty queries. They also proposed a new MAC scheme, dubbed nEHtM, and showed that it enjoys graceful degradation of security in this model. The two models of nonce misuse above seem to complement each other; when an m-multicollsion of a single nonce happens, it implies that there have been at least $m-1$ faulty queries, while any number of faulty queries can be made by multicollisions of nonces with small multiplicities.

Birthday and Beyond-Birthday Security. Most block cipher-based AE modes provide only the birthday-bound security (with respect to the size of the underlying primitive). For example, if an AE mode is based on a 128-bit block cipher such as AES, then it would guarantee only up to 64-bit security, whereas this bound might not be sufficient in defense-in-depth applications where higher security is required.

Some AE schemes enjoy beyond-birthday-bound security. Iwata [13] proposed the CIP AE mode of rate 4/9 (for the default parameters) and $2n/3$-bit security, and Iwata and Minematsu [14] proposed a variant of GCM-SIV of rate 1/4 and $2n/3$-bit security. Bose et al. [4] proved n-bit security of AES-GCM-SIV in the ideal cipher model. However, in this stronger model, its provable security would not be called "full" since the underlying ideal primitive accepts $(n+\kappa)$-bit inputs, where κ denotes the key size. Assuming the multi-user security of AES in the

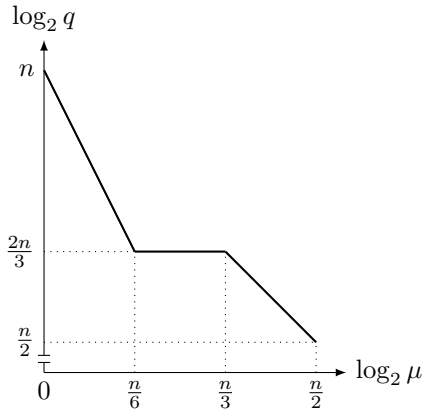


Fig. 1: Security of SCM in terms of the threshold number of encryption queries q as a function of the number of faulty queries μ.

standard model, Iwata and Seurin [16] proved $3n/4$-bit security of AES-GCM-SIV. The mGCM mode [3] achieves almost n-bit security with reasonable efficiency (of rate around 1/2) in the standard model, while it is vulnerable to nonce misuse.

When it comes to *tweakable* block cipher-based constructions (for simplicity, assuming that the underlying tweakable block cipher uses n-bit tweaks), SCT [24] provides n-bit security in the nonce-respecting setting, while its integrity falls down to the birthday bound as soon as a nonce is repeated. Iwata et al. proposed ZAE [15], which is a deterministic AE scheme providing n-bit security.

The focus of this paper is put on the construction of (conventional) block cipher-based *nonce-misuse resistant* AE schemes with almost n-bit security and reasonable efficiency assuming the *pseudorandomness* of the underlying block cipher in the single-user setting. One of the advantages of block cipher-based schemes is that it can be instantiated with a widely-used block cipher such as AES. Due to AES-NI instructions, and a considerable amount of research on efficient implementation of AES, AES-based schemes are usually faster than tweakable block cipher-based ones. On the other hand, compared to using an n-bit tweakable block cipher, it seems more challenging to achieve the same level of security using an n-bit conventional block cipher with a weaker security assumption.

1.1 Our Contribution

We propose the Synthetic Counter with Masking (SCM) mode, which turns a block cipher into a nonce-based authenticated encryption scheme. SCM follows the NSIV paradigm proposed by Peyrin and Seurin in CRYPTO 2016 [24], where a keyed hash function accepts a nonce N with associated data and a message, yielding an authentication tag T, and then the message is encrypted by a counter-like mode using both T and N. Here we move one step further by *encrypting*

AEAD	Assumption	Rate	Security		Graceful degradation	Reference
			NR	NM		
GCM	PRF	1/2	$n/2$	–	✗	[20]
OCB3	PRP	1	$n/2$	–	✗	[18]
mGCM	PRP	1/2	n	–	✗	[3]
GCM-SIV	PRF	1/2	$n/2$	$n/2$	✓	[10]
CWC+	PRP	1/2	$3n/4$	$n/2^{\dagger}$	✓†	[8]
AES-GCM-SIV	muPRP	1/2	$3n/4$	$n/2$	✓	[16]
AES-GCM-SIV‡	ICM	1/2	n	$n/2$	✓	[4]
SCM	PRP	1/2	n	$n/2$	✓	This work
ΘCB	TPRP	1	n	–	✗	[18]
SCT	TPRP	1/2	n	$n/2$	✗	[24]
ZAE	TPRP	2/3	n	n	✓	[15]

† Authenticity only. CWC+ does not provide privacy in the nonce-misuse setting.
‡ A variant of AES-GCM-SIV with the key derivation function modified.

Table 1: Comparison of SCM with existing AE modes. NR (resp. NM) represents the nonce-respecting setting (resp. the nonce-misuse setting).

nonces: from a secret key and a nonce, three encrypted nonces Δ, Δ' and Δ'' are computed. The authentication tag T is defined by a variant of nEHtM [8] using Δ''. More precisely, for an associated data A and a message M,

$$T = E_{K'}(H_{K_h}(A, M) \oplus (N \,\|\, 00)) \oplus \Delta''.$$

The i-th keystream block $Z[i]$ is defined as

$$Z[i] = E_K(T \oplus 2^{i-1}\Delta) \oplus \Delta',$$

which is xored to the corresponding message block. We prove that if H is a δ-almost XOR universal hash function with $\delta \approx \frac{1}{2^n}$, if E is a secure block cipher, and if the maximum length of encryption queries is sufficiently small, then SCM is secure up to $O(2^n)$ encryption and decryption queries in the nonce-respecting setting. Even if nonces are repeated, SCM is secure up to the birthday bound, enjoying graceful security degradation in the faulty nonce model. Figure 1 shows the security bounds of SCM in terms of the threshold number of encryption queries q as a function of the number of faulty queries μ ignoring the maximum message length. The influence of μ to the threshold number of decryption queries is negligible as seen in Theorem 1 (with $L = n$).

Table 1 compares SCM to well-known AE schemes based on (tweakable) block ciphers. For simplicity of comparison, we assume that the underlying tweakable block cipher uses n-bit tweaks. To the best of our knowledge, SCM is the first block cipher-based nonce-misuse resistant AE scheme of rate 1/2 that provides n-bit security in the nonce-respecting setting when the underlying n-bit block cipher is modeled as a pseudorandom permutation. Seen as a slight variant of GCM-SIV, SCM is also parallelizable and inverse-free.

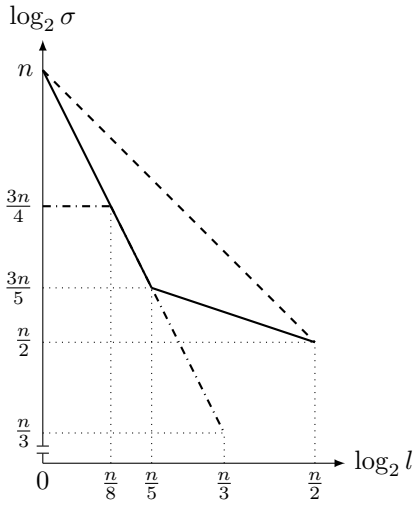


Fig. 2: The threshold number of the total length of the encryption queries σ as a function of l, where the number of faulty queries μ is fixed as a small constant. The solid line is the bound for SCM, while the dashed (resp. dash-dotted) line is the bound for AES-GCM-SIV in the ideal cipher (resp. multi-user PRP) model.

Figure 2 compares the influence of the maximum message length l to the threshold number of the total length of the encryption queries σ for SCM and AES-GCM-SIV, where we distinguish two different models in which AES-GCM-SIV has been analyzed. When security bounds are not represented by only σ and l, we use a (loose) bound $q \leq \sigma$. We see that SCM provides stronger bounds than AES-GCM-SIV in the standard model. We note that GCM, OCB3 and GCM-SIV are secure when $\sigma \ll 2^{\frac{n}{2}}$, while all the tweakble cipher-based constructions ΘCB, SCT, and ZAE are secure when $\sigma \ll 2^n$, all regardless of the maximum message length. In [8], CWC+ has been proved to be secure up to $2^{\frac{2n}{3}}$ block cipher queries, while one can obtain a stronger bound using recent results [3, 5]. Even with this improvement, its security does not go beyond $2^{\frac{3n}{4}}$ (in terms of σ).

Being nonce-misuse resistant, SCM provides beyond-birthday-bound security as long as $\mu l \ll 2^{n/2}$, and it can be seen as optimal when μ and l are small enough. This property is practically relevant for a certain case, where data is broken into small parts, and they are encrypted with different nonces. For example, in the TLS network protocol, the maximum transmission unit (MTU) is typically set to 1500B, and each fragment is encrypted with a different nonce using its sequence number.

Table 2 compares SCM using POLYVAL[1] [9] as a universal hash function to existing AE schemes in terms of efficiency. In this comparison, we focus on the AE schemes whose reference codes are publicly available (except ZAE). The efficiency of ZAE has been only approximately estimated based on the speed

[1] POLYVAL is a universal hash function used in AES-GCM-SIV

Mode	Cipher	Message			Reference
		1KB	4KB	64KB	
ChaCha20-Poly1305	-	2.17	1.55	1.47	[21]
GCM	AES-128	1.23	0.63	0.56	[20]
AES-GCM-SIV	AES-128	1.57	0.89	0.81	[16]
Deoxys-I ($\approx$ ΘCB)	Deoxys-BC-256	1.38	0.91	0.77	[17]
Deoxys-II ($\approx$ SCT)	Deoxys-BC-256	2.19	1.68	1.52	[17]
ZAE	Deoxys-BC-256	$\geq$1.94	$\geq$1.41	$\geq$1.25	[15]
SCM	AES-128	0.94	0.86	0.83	This work

Table 2: Performance comparison of SCM to various AE schemes. Throughput is measured in cycles per byte.

of Deoxys-BC-256 in counter mode (as done in [15]), so the number in Table 2 should be understood as rough lower bounds. The implementations of ChaCha20-Poly1305, GCM, and AES-GCM-SIV are taken from BoringSSL[2] and those of Deoxys-I and Deoxys-II are taken from SUPERCOP[3]. Our experiments are done in the Skylake microarchitecture (i7-6700 CPU@4.20GHz) which supports PCLMUL, AVX, SSE, and AES instructions, using GCC 7.4.0 with optimization level -O2.

Although SCM requires four block cipher calls to encrypt nonces at the beginning of every encryption, our implementation shows that it does not slow down the overall efficiency since it can be done in parallel with the encryption of the hash output. We see that SCM is comparable to AES-GCM-SIV.

Overview of the Proof. Our security proof takes a modular approach; $\mathsf{SCM}[H, E]$ (based on a keyed hash function H and a block cipher E) is decomposed into a MAC scheme and an encryption scheme, denoted $\mathsf{SCM.MAC}[H, E]$ and $\mathsf{SCM.PRNG}[E]$, respectively. We first prove that if both $\mathsf{SCM.MAC}[H, E]$ and $\mathsf{SCM.PRNG}[E]$ are secure, then $\mathsf{SCM}[H, E]$ is also secure (Lemma 5), where we need to slightly modify the security model for the encryption part; it takes as input a random tag T (which can be seen as an initial vector), and T is also given to the adversary.

The underlying MAC scheme is similar to the nonce-based enhanced hash-then-mask MAC (nEHtM), whose security has been recently proved up to $2^{\frac{3n}{4}}$ MAC queries [5]. The main difference of SCM.MAC from nEHtM is that the "encrypted mask" $E_K(N)$ used in nEHtM is replaced by $E_K(N\|00)\oplus E_K(N\|11)$ using an $(n-2)$-bit nonce N, which can be seen as $\rho(N)$ for a truly random function ρ. At the cost of an additional block cipher call, $\mathsf{SCM.MAC}[H, E]$ is secure up to 2^n MAC queries when H is a δ-almost XOR universal with $\delta \approx \frac{1}{2^n}$ (Lemma 6).

[2] https://boringssl.googlesource.com/boringssl
[3] https://bench.cr.yp.to/supercop.html

The pseudorandomness of $\mathsf{SCM.PRNG}[E]$ is analyzed by two different approaches. When the number of faulty queries μ is relatively large, we use Mirror theory in a refined form as given in [5] (and restated in Lemma 3). In Lemma 7, we prove that $\mathsf{SCM.PRNG}[E]$ is pseudorandom up to $2^{\frac{2n}{3}}$ queries, enjoying graceful security degradation as μ increases.

When μ is small, for example, in the nonce-respecting setting, one can expect even stronger security. In such cases, we make the adversary *non-adaptive* by allowing it to repeat each nonce exactly μ times. In this setting, we can use the χ^2-method as restated in Lemma 2, and its interpretation in terms of Mirror theory as given in Lemma 4. All the bounds contain the sum-of-squares and sum-of-cubes of component sizes in the graph representation of the transcript, and it is the most challenging part of the proof to upper bound their expectation (Lemma 11 and 13). Finally, we apply the expectation method to prove the security of $\mathsf{SCM.PRNG}[E]$ up to 2^n queries in the nonce-respecting setting (Lemma 8).

2 Preliminaries

2.1 Notation

In all of the following, we fix a positive integer n such that $n \geq 3$. We denote 0^n (i.e., n-bit string of all zeros) by $\mathbf{0}$. The set $\{0,1\}^n$ is sometimes regarded as a set of integers $\{0, 1, \ldots, 2^n - 1\}$ by converting an n-bit string $a_{n-1} \cdots a_1 a_0 \in \{0,1\}^n$ to an integer $a_{n-1}2^{n-1} + \cdots + a_1 2 + a_0$. We also identify $\{0,1\}^n$ with a finite field $\mathbf{GF}(2^n)$ with 2^n elements, assuming that 2 cyclically generates all the nonzero elements of $\mathbf{GF}(2^n)$. We write $\{0,1\}^*$ to denote the set of all binary strings including the empty string. For $X \in \{0,1\}^*$, $|X|$ denotes its length. For a nonnegative integer s and a string $X \in \{0,1\}^*$ such that $|X| \leq s$, $\mathsf{msb}_s(X)$ denotes the s most significant bits of X. For a positive integer q, we write $[q] = \{1, \ldots, q\}$.

Given a non-empty finite set $\mathcal{X}$, $x \leftarrow_{\$} \mathcal{X}$ denotes that x is chosen uniformly at random from $\mathcal{X}$. The set of all functions from $\mathcal{X}$ to $\mathcal{Y}$ is denoted $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$, and the set of all permutations of $\mathcal{X}$ is denoted $\mathsf{Perm}(\mathcal{X})$. The set of all permutations of $\{0,1\}^n$ is simply denoted $\mathsf{Perm}(n)$. The set of all sequences that consist of b pairwise distinct elements of $\mathcal{X}$ is denoted $\mathcal{X}^{*b}$. For integers $1 \leq b \leq a$, we will write $(a)_b = a(a-1)\cdots(a-b+1)$ and $(a)_0 = 1$ by convention. If $|\mathcal{X}| = a$, then $(a)_b$ becomes the size of $\mathcal{X}^{*b}$.

When two sets $\mathcal{X}$ and $\mathcal{Y}$ are disjoint, their (disjoint) union is denoted $\mathcal{X} \sqcup \mathcal{Y}$. For a set $\mathcal{X} \subset \{0,1\}^n$ and $\lambda \in \{0,1\}^n$, we will write $\mathcal{X} \oplus \lambda = \{x \oplus \lambda : x \in \mathcal{X}\}$. For a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, we will interchangeably write $|\mathcal{V}|$ and $|\mathcal{G}|$ for the number of vertices of $\mathcal{G}$.

2.2 Security Notions

Almost Xor Universal Hash Functions. Let $\delta > 0$, and let $H : \mathcal{K}_h \times \mathcal{M} \to \mathcal{X}$ be a keyed function for three non-empty sets $\mathcal{K}_h$, $\mathcal{M}$, and $\mathcal{X}$. H is said to be

δ-almost XOR universal (AXU) if for any distinct $M, M' \in \mathcal{M}$ and $X \in \mathcal{X}$,

$$\Pr\left[K_h \leftarrow_{\$} \mathcal{K}_h : H_{K_h}(M) \oplus H_{K_h}(M') = X\right] \leq \delta.$$

PRPs. Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a keyed permutation with key space $\mathcal{K}$, where $E(K,\cdot)$ is a permutation for each $K \in \mathcal{K}$. We will denote $E_K(X)$ for $E(K,X)$. A (q,t)-distinguisher against E is an algorithm $\mathcal{D}$ with oracle access to an n-bit permutation and its inverse, making at most q oracle queries, running in time at most t, and outputting a single bit. The advantage of $\mathcal{D}$ in breaking the PRP-security of E, i.e., in distinguishing E from a uniform random permutation $\pi \leftarrow_{\$} \mathsf{Perm}(n)$, is defined as

$$\mathsf{Adv}^{\mathsf{prp}}_E(\mathcal{D}) = \left|\Pr\left[K \leftarrow_{\$} \mathcal{K} : \mathcal{D}^{E_K, E_K^{-1}} = 1\right] - \Pr\left[\pi \leftarrow_{\$} \mathsf{Perm}(n) : \mathcal{D}^{\pi,\pi^{-1}} = 1\right]\right|.$$

We define $\mathsf{Adv}^{\mathsf{prp}}_E(q,t)$ as the maximum of $\mathsf{Adv}^{\mathsf{prp}}_E(\mathcal{D})$ over all (q,t)-distinguishers against E.

Nonce-based MACs. Given four non-empty sets $\mathcal{K}$, $\mathcal{N}$, $\mathcal{M}$, and $\mathcal{T}$, a nonce-based MAC with key space $\mathcal{K}$, nonce space $\mathcal{N}$, message space $\mathcal{M}$ and tag space $\mathcal{T}$ is a function $F : \mathcal{K} \times \mathcal{N} \times \mathcal{M} \to \mathcal{T}$. Stated otherwise, it is a keyed function whose domain is a cartesian product $\mathcal{N} \times \mathcal{M}$. We will sometimes write $F_K(N,M)$ to denote $F(K,N,M)$.

For $K \in \mathcal{K}$, let Auth_K be the MAC oracle which takes as input a pair $(N,M) \in \mathcal{N} \times \mathcal{M}$ and returns $F_K(N,M)$, and let Ver_K be the verification oracle which takes as input a triple $(N,M,T) \in \mathcal{N} \times \mathcal{M} \times \mathcal{T}$ and returns $\top$ ("accept") if $F_K(N,M) = T$, and $\bot$ ("reject") otherwise. We assume that an adversary makes queries to the two oracles Auth_K and Ver_K for a secret key $K \in \mathcal{K}$. A MAC query (N,M) made by an adversary is called a *faulty query* if the adversary has already queried to the MAC oracle with the same nonce but with a different message. For example, if the i-th query is denoted by (N_i, M_i) and there are four distinct queries, (N_i, M_i) for $i \in [4]$ such that $N_1 \neq N_2 = N_3 = N_4$, the third and the fourth queries are faulty and the number of faulty queries is two.

In this work, we will consider the MAC security of F using the advantage of an adversary trying to distinguish the real world $(\mathsf{Auth}_K, \mathsf{Ver}_K)$ and the ideal world. The ideal world oracles are $(\mathsf{Rand}, \mathsf{Rej})$, where Rand returns an independent random value (instantiating a truly random function) and Rej always returns $\bot$ for every verification query. A (μ,q,v,t)-distinguisher against the MAC security of F is an algorithm $\mathcal{D}$ with oracle access to $\mathsf{Auth}_K/\mathsf{Rand}$ and $\mathsf{Ver}_K/\mathsf{Rej}$, making at most q MAC queries to its first oracle with at most μ faulty queries and at most v verification queries to its second oracle, and running in time at most t. We assume that $\mathcal{D}$ does not make a verification query by reusing any previous MAC query. We define

$$\mathsf{Adv}^{\mathsf{mac}}_F(\mu,q,v,t) = \max_{\mathcal{D}}\left(\Pr\left[K \leftarrow_{\$} \mathcal{K} : \mathcal{D}^{\mathsf{Auth}_K, \mathsf{Ver}_K} = 1\right] - \Pr\left[\mathcal{D}^{\mathsf{Rand},\mathsf{Rej}} = 1\right]\right),$$

where the maximum is taken over all (μ,q,v,t)-distinguishers $\mathcal{D}$. When we consider information theoretic security, we will drop the parameter t.

NONCE-BASED AE SCHEMES. Given four non-empty sets $\mathcal{K}$, $\mathcal{N}$, $\mathcal{A}$ and $\mathcal{M}$, a nonce-based authenticated encryption (AE) scheme is a tuple

$$\Pi = (\mathcal{K}, \mathcal{N}, \mathcal{A}, \mathcal{M}, \mathsf{Enc}, \mathsf{Dec}),$$

where Enc and Dec are called encryption and decryption algorithms, respectively. The encryption algorithm Enc takes as input a key $K \in \mathcal{K}$, a nonce $N \in \mathcal{N}$, an associated data $A \in \mathcal{A}$, and a message $M \in \mathcal{M}$, and outputs a ciphertext $C \in \{0,1\}^*$. The decryption algorithm Dec takes as input a tuple $(K, N, A, C) \in \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \{0,1\}^*$, and outputs either a message $M \in \mathcal{M}$ or a special symbol $\perp$. We require that

$$\mathsf{Dec}(K, N, A, \mathsf{Enc}(K, N, A, M)) = M$$

for any tuple $(K, N, A, M) \in \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M}$. We will write $\mathsf{Enc}_K(N, A, M)$ and $\mathsf{Dec}_K(N, A, C)$ to denote $\mathsf{Enc}(K, N, A, M)$ and $\mathsf{Dec}(K, N, A, C)$, respectively.

The goal of an adversary $\mathcal{D}$ against the nonce-based AE security of Π is to distinguish the real world $(\mathsf{Enc}_K, \mathsf{Dec}_K)$ (using a random key K, unknown to $\mathcal{D}$) and the ideal world. The ideal world oracles are $(\mathsf{Rand}, \mathsf{Rej})$, where Rand returns an independent random string of length $|\mathsf{Enc}_K(N, A, M)|$ and Rej always returns $\perp$ for every decryption query. We assume that $\mathcal{D}$ does not make a decryption query by reusing any previous encryption query. The advantage of $\mathcal{D}$ breaking the nAE-security of Π is defined as

$$\mathsf{Adv}^{\mathsf{nAE}}_{\Pi}(\mathcal{D}) = \left|\Pr\left[K \leftarrow_{\$} \mathcal{K} : \mathcal{D}^{\mathsf{Enc}_K, \mathsf{Dec}_K} = 1\right] - \Pr\left[\mathcal{D}^{\mathsf{Rand}, \mathsf{Rej}} = 1\right]\right|.$$

A $(\mu, q, v, \sigma, l, t)$-adversary against the nonce-based AE security of Π is an algorithm that makes at most q encryption queries to its first oracle with at most μ faulty queries (using repeated nonces) and at most v decryption queries to its second oracle, and running in time at most t, where the length of each encryption/decryption query is at most l blocks of n bits, and the total length of the encryption queries (nonce excluded) is at most σ blocks of n bits. When $\mu = 0$, we say that $\mathcal{D}$ is nonce-respecting, otherwise $\mathcal{D}$ is said nonce-misusing. However, the adversary is allowed to repeat nonces in its Dec oracle. We define $\mathsf{Adv}^{\mathsf{nAE}}_{\Pi}(\mu, q, v, \sigma, l, t)$ as the maximum of $\mathsf{Adv}^{\mathsf{nAE}}_{\Pi}(\mathcal{D})$ over all $(\mu, q, v, \sigma, l, t)$-adversaries $\mathcal{D}$ against Π. When we consider information theoretic security, we will drop the parameter t.

2.3 Coefficient-H Technique

We will use Patarin's coefficient-H technique, more precisely, its refinement called the *expectation method* [12]. The goal of this technique is to upper bound the adversarial distinguishing advantage between a real construction and its ideal counterpart. In the real and the ideal worlds, an information-theoretic adversary $\mathcal{D}$ is allowed to make queries to certain oracles (with the same oracle interfaces), denoted $\mathcal{O}_{\mathsf{real}}$ and $\mathcal{O}_{\mathsf{ideal}}$, respectively. The interaction between the adversary $\mathcal{D}$ and the oracle determines a "transcript"; it contains all the information obtained

by $\mathcal{D}$ during the interaction. We call a transcript τ *attainable* if the probability of obtaining τ in the ideal world is non-zero. We also denote T_{id}(resp. T_{re}) the probability distribution of the transcript τ induced by the ideal world (resp. the real world). By extension, we use the same notation to denote a random variable distributed according to each distribution.

We partition the set of attainable transcripts Γ into a set of "good" transcripts Γ_{good} such that the probabilities to obtain some transcript $\tau \in \Gamma_{\mathsf{good}}$ are close in the real world and the ideal world, and a set Γ_{bad} of "bad" transcripts such that the probability to obtain any $\tau \in \Gamma_{\mathsf{bad}}$ is small in the ideal world. The lower bound in the ratio of the probabilities to obtain a good transcript in both worlds will be given as a function of τ, and we will take its expectation. The expectation method is summarized in the following lemma.

Lemma 1. *Let $\Gamma = \Gamma_{\mathsf{good}} \sqcup \Gamma_{\mathsf{bad}}$ be a partition of the set of attainable transcripts, where there exists a non-negative function $\varepsilon_1(\tau)$ such that for any $\tau \in \Gamma_{\mathsf{good}}$,*

$$\frac{\Pr\left[\mathsf{T}_{\mathrm{re}} = \tau\right]}{\Pr\left[\mathsf{T}_{\mathrm{id}} = \tau\right]} \geq 1 - \varepsilon_1(\tau),$$

and there exists ε_2 such that $\Pr[\mathsf{T}_{\mathrm{id}} \in \Gamma_{\mathsf{bad}}] \leq \varepsilon_2$. Then for any adversary $\mathcal{D}$,

$$\left|\Pr\left[\mathcal{D}^{\mathcal{O}_{\mathsf{real}}} = 1\right] - \Pr\left[\mathcal{D}^{\mathcal{O}_{\mathsf{ideal}}} = 1\right]\right| \leq \mathsf{Ex}\left[\varepsilon_1(\tau)\right] + \varepsilon_2,$$

where the expectation is taken over the distribution T_{id} in the ideal world.

Proof. Since the distinguisher's output is a (deterministic) function of the transcript, its distinguishing advantage is upper bounded by the statistical distance between T_{id} and T_{re}. So we have

$$\begin{aligned}\left|\Pr\left[\mathcal{D}^{\mathcal{O}_{\mathsf{real}}} = 1\right] - \Pr\left[\mathcal{D}^{\mathcal{O}_{\mathsf{ideal}}} = 1\right]\right| &\leq \|\mathsf{T}_{\mathrm{re}} - \mathsf{T}_{\mathrm{id}}\| \\ &\stackrel{\text{def}}{=} \frac{1}{2}\sum_{\tau \in \Gamma} \left|\Pr[\mathsf{T}_{\mathrm{re}} = \tau] - \Pr[\mathsf{T}_{\mathrm{id}} = \tau]\right|.\end{aligned}$$

Moreover we have:

$$\begin{aligned}\|\mathsf{T}_{\mathrm{re}} - \mathsf{T}_{\mathrm{id}}\| &= \sum_{\substack{\tau \in \Gamma \\ \Pr[\mathsf{T}_{\mathrm{id}} = \tau] > \Pr[\mathsf{T}_{\mathrm{re}} = \tau]}} \left(\Pr[\mathsf{T}_{\mathrm{id}} = \tau] - \Pr[\mathsf{T}_{\mathrm{re}} = \tau]\right) \\ &= \sum_{\substack{\tau \in \Gamma \\ \Pr[\mathsf{T}_{\mathrm{id}} = \tau] > \Pr[\mathsf{T}_{\mathrm{re}} = \tau]}} \Pr[\mathsf{T}_{\mathrm{id}} = \tau]\left(1 - \frac{\Pr[\mathsf{T}_{\mathrm{re}} = \tau]}{\Pr[\mathsf{T}_{\mathrm{id}} = \tau]}\right) \\ &\leq \sum_{\tau \in \Gamma_{\mathsf{good}}} \Pr[\mathsf{T}_{\mathrm{id}} = \tau]\varepsilon_1(\tau) + \sum_{\tau \in \Gamma_{\mathsf{bad}}} \Pr[\mathsf{T}_{\mathrm{id}} = \tau] \\ &\leq \mathsf{Ex}[\varepsilon_1(\tau)] + \varepsilon_2.\end{aligned}$$

□

2.4 Sampling with Replacement Using a Random Permutation

Xoring the outputs of a random permutation is a simple way of generating pseudorandom samples using a random permutation. A random permutation can be viewed as a random sampling *without replacement*.

Fix positive integers $w_1, \ldots, w_r \geq 2$. Let $\sigma = \sum_{i \in [r]} w_i$, and let

$$\mathsf{T} = (T_{i,j})_{i \in [r], j \in [w_i]} = (T_{1,1}, \cdots, T_{1,w_1}, T_{2,1}, \cdots, T_{2,w_2}, \cdots, T_{r,1}, \cdots, T_{r,w_r})$$

be a sequence sampled from $(\{0,1\}^n)^{*\sigma}$ uniformly at random (i.e., by random sampling without replacement). Let

$$\begin{aligned}\mathsf{S} &= (T_{i,j} \oplus T_{i,w_i})_{i \in [r], j \in [w_i - 1]} \\ &= (T_{1,1} \oplus T_{1,w_1}, \cdots, T_{1,w_1 - 1} \oplus T_{1,w_1}, \cdots, T_{r,1} \oplus T_{r,w_r}, \cdots, T_{r,w_r - 1} \oplus T_{r,w_r})\end{aligned}$$

Using the χ^2-method, Bhattacharya and Nandi [3] proved the pseudorandomness of S as follows.

Lemma 2. *Let S be a sequence sampled as described above, and let R be a sequence sampled from $(\{0,1\}^n)^{\sigma - r}$ uniformly at random.*[4] *Then we have*

$$\|\mathsf{S} - \mathsf{R}\| \leq \left(\frac{4\sigma}{2^{2n}} \sum_{i=1}^{r} w_i^3 \right)^{\frac{1}{2}} + \sum_{i=1}^{r} \frac{w_i(w_i - 1)}{2^{n+1}}. \tag{1}$$

For an integer $w \geq 2$, let $w_i = w$ for $i \in 1, \ldots, r$. Then we have

$$\|\mathsf{S} - \mathsf{R}\| \leq \frac{\sqrt{2} r w^2}{2^n} + \frac{w(w-1)r}{2^{n+1}}. \tag{2}$$

We note that (2) is simply a restatement of Theorem 2 in [3], and (1) can also be derived from the proof of the theorem (see page 327 in [3]).

2.5 Mirror Theory

Mirror theory [22, 23] is one of the main tools for our security proof, whose goal is to systematically estimate the number of solutions to a system of equations. Mirror theory is later generalized to *extended* Mirror theory [6, 8], by including non-equations in the system.

A system of equations and non-equations can be represented by a graph. Each vertex corresponds to an n-bit *distinct* unknowns. By abuse of notation, we will identify the vertices with the values assigned to them. We distinguish two types of edges, namely, $=$-labeled edges and $\neq$-labeled edges that correspond to equations and non-equations, respectively. So we consider a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}^{=} \sqcup \mathcal{E}^{\neq})$, where $\mathcal{E}^{=}$ and $\mathcal{E}^{\neq}$ denote the set of $=$-labeled edges and the set of $\neq$-labeled edges,

[4] We will view S and R as random variables, and also write them to denote their probability distributions.

respectively. Then $\mathcal{G}$ can be seen as a superposition of two subgraphs $\mathcal{G}^{=} =^{\text{def}} (\mathcal{V}, \mathcal{E}^{=})$ and $\mathcal{G}^{\neq} =^{\text{def}} (\mathcal{V}, \mathcal{E}^{\neq})$.

We will define *label functions* $\lambda : \mathcal{E}^{=} \to \{0,1\}^n$ and $\lambda' : \mathcal{E}^{\neq} \to \{0,1\}^n$. If two vertices P and Q are adjacent by an $=$-labeled (resp. $\neq$-labeled) edge and $\lambda(P,Q) = c$ (resp. $\lambda'(P,Q) = c$) for some $c \in \{0,1\}^n$, then it would mean that $P \oplus Q = c$ (resp. $P \oplus Q \neq c$). We will write $h(\mathcal{G}, \lambda, \lambda')$ to denote the number of solutions to $(\mathcal{G}, \lambda, \lambda')$ such that all the vertices take different values in $\{0,1\}^n$. When there is no $\neq$-labeled edge, we will simply write $h(\mathcal{G}, \lambda)$.

Throughout this paper, we will consider a graph $\mathcal{G}$ such that $\mathcal{G}^{=}$ has no cycle. In this case, $\mathcal{G}^{=}$ is decomposed into its connected components, all of which are trees; let

$$\mathcal{G}^{=} = \mathcal{C}_1 \sqcup \mathcal{C}_2 \sqcup \cdots \sqcup \mathcal{C}_r \sqcup \mathcal{D} \tag{3}$$

for some $r \geq 0$, where $\mathcal{C}_i$ denotes a component of size at least 2, and $\mathcal{D}$ denotes the set of *isolated* vertices. Any pair of distinct vertices P and Q in the same component are connected by a unique trail,[5] say,

$$P = P_0 - P_1 - \cdots - P_s = Q.$$

In this case, we define

$$\bar{\lambda}(P,Q) \stackrel{\text{def}}{=} \sum_{i=0}^{r-1} \lambda(P_i, P_{i+1}).$$

By defining $\bar{\lambda}(P,Q) = \perp$ for any pair of vertices P and Q contained in different components, $\bar{\lambda}$ is defined on $\mathcal{V}^{*2}$, extending λ. For $\mathcal{G} = (\mathcal{V}, \mathcal{E}^{=} \cup \mathcal{E}^{\neq})$, let

$$\mathcal{L}(\mathcal{G}) \stackrel{\text{def}}{=} \mathsf{Func}(\mathcal{E}^{=}, \{0,1\}^n) \times \mathsf{Func}(\mathcal{E}^{\neq}, \{0,1\}^n).$$

We call $(\lambda, \lambda') \in \mathcal{L}(\mathcal{G})$ *bad* if one of the following conditions holds:

- there exists $(P,Q) \in \mathcal{V}^{*2}$ such that $\bar{\lambda}(P,Q) = \mathbf{0}$;
- there exists $(P,Q) \in \mathcal{E}^{\neq}$ such that $\bar{\lambda}(P,Q) = \lambda'(P,Q)$.

Note that $h(\mathcal{G}, \lambda, \lambda') = 0$ if (λ, λ') is bad. Let $\mathcal{L}_{\mathsf{bad}}(\mathcal{G})$ denote the set of the bad label functions in $\mathcal{L}(\mathcal{G})$. When $(\lambda, \lambda') \notin \mathcal{L}_{\mathsf{bad}}(\mathcal{G})$, we can lower bound $h(\mathcal{G}, \lambda, \lambda')$ using the extended Mirror theory as follows.

Lemma 3. *For positive integers q and v, let $\mathcal{G} = (\mathcal{V}, \mathcal{E}^{=} \cup \mathcal{E}^{\neq})$ be a graph such that $\mathcal{G}^{=}$ has no cycle, $|\mathcal{V}| \leq 2^n$, $|\mathcal{E}^{=}| = q$, and $|\mathcal{E}^{\neq}| = v$. Suppose that $\mathcal{G}^{=}$ is decomposed into its connected components as in (3). Let $w_i = |\mathcal{C}_i|$ for $i = 1, \ldots, r$, and let $\sigma = \sum_{i=1}^{r} w_i$. Then, for any $(\lambda, \lambda') \notin \mathcal{L}_{\mathsf{bad}}(\mathcal{G})$, we have*

$$\frac{h(\mathcal{G}, \lambda, \lambda')}{(2^n)_{|\mathcal{V}|}} \geq \frac{1}{2^{qn}} \left(1 - \frac{\sigma^2}{2^{2n}} \sum_{i=1}^{r} w_i^2 - \frac{2v}{2^n}\right).$$

[5] A trail is a walk in which all edges are distinct.

Proof. For $i = 1, \ldots, r$,

- let $\sigma_i = \sum_{j=1}^{i} w_j$;
- let $\mathcal{G}_i = (\mathcal{V}_i, \mathcal{E}_i)$ be the graph obtained from $\mathcal{C}_1 \sqcup \mathcal{C}_2 \sqcup \cdots \sqcup \mathcal{C}_i$ by adding all the $\neq$-labeled edges connecting the vertices in $\mathcal{C}_1 \sqcup \mathcal{C}_2 \sqcup \cdots \sqcup \mathcal{C}_i$;
- let v_i be the number of $\neq$-labeled edges that connect a vertex in $\mathcal{C}_i$ and one in $\mathcal{G}_{i-1}$;
- let $h(i)$ be the number of solutions to $(\mathcal{G}_i, \lambda, \lambda')$ (with the domains of λ and λ' restricted to $\mathcal{G}_i$).

Let $h(0) = 1$ and let $\sigma_0 = 0$. Note that $\mathcal{G} = \mathcal{G}_r \sqcup \mathcal{D}$. If there exists $i \in [r-1]$ such that $\sigma_i w_{i+1} > 2^n$, we get

$$\sigma^2 w_{i+1}^2 \geq \sigma_i^2 w_{i+1}^2 > 2^{2n}$$

so the lemma trivially holds. Therefore, let us assume that for $i = 0, \ldots, r-1$, $\sigma_i w_{i+1} \leq 2^n$. Similarly, we can assume that $\sigma \leq 2^{n-1}$. In order to find a relation between $h(i)$ and $h(i+1)$, we fix a solution to $\mathcal{G}_i$. If we fix a vertex $V^* \in \mathcal{V}_{i+1}$ and assign any value to V^*, then the other unknowns in $\mathcal{V}_{i+1}$ are uniquely determined, since there is a unique trail from V^* to any other vertices in $\mathcal{V}_{i+1}$. In order to make all assigned values distinct, it is sufficient that

$$V^* \notin \bigcup_{X \in \mathcal{V}_{i+1}} \left((\mathcal{V}_1 \sqcup \cdots \sqcup \mathcal{V}_i) \oplus \bar{\lambda}(V^*, X) \right).$$

Moreover, V^* should satisfy v_{i+1} non-equations. The number of possible choices satisfying these conditions is at least $2^n - \sigma_i w_{i+1} - v_{i+1}$, which means

$$h(i+1) \geq (2^n - \sigma_i w_{i+1} - v_{i+1}) h(i).$$

Then for $0 \leq i \leq r-1$, we have

$$\begin{aligned}
\frac{h(i+1) 2^{n(w_{i+1}-1)}}{h(i)(2^n - \sigma_i)_{w_{i+1}}} &\geq \frac{h(i+1)}{h(i)} \cdot \frac{1}{2^n} \left(\frac{2^n}{2^n - \sigma_i} \right)^{w_{i+1}} \\
&\geq \frac{h(i+1)}{h(i)} \cdot \frac{1}{2^n} \left(1 + \frac{\sigma_i}{2^n} \right)^{w_{i+1}} \\
&\geq \left(1 - \frac{\sigma_i w_{i+1}}{2^n} - \frac{v_{i+1}}{2^n} \right) \left(1 + \frac{\sigma_i w_{i+1}}{2^n} \right) \\
&\geq 1 - \frac{\sigma_i^2 w_{i+1}^2}{2^{2n}} - \frac{2 v_{i+1}}{2^n}
\end{aligned}$$

since $\sigma_i w_{i+1} \leq 2^n$.

Let v_D denote the number of $\neq$-labeled edges that are incident to some vertex in $\mathcal{D}$. For any fixed solution to $\mathcal{G}_r$, the number of possible assignments of distinct values to the vertices of $\mathcal{D}$ is $(2^n - \sigma)_{|\mathcal{D}|}$. Among these assignments, at most $(2^n - \sigma - 1)_{|D|-1}$ assignments violate any fixed $\neq$-labeled edge that connects $\mathcal{D}$ and $\mathcal{G}_r$. Therefore, we have

$$h(\mathcal{G}, \lambda, \lambda') \geq \left((2^n - \sigma)_{|\mathcal{D}|} - v_D (2^n - \sigma - 1)_{|\mathcal{D}|-1} \right) h(r),$$

which means

$$\frac{h(\mathcal{G},\lambda,\lambda')}{(2^n-\sigma)_{|\mathcal{D}|}h(r)} \geq 1-\frac{2v_D}{2^n}$$

since $\sigma \leq 2^{n-1}$. Since $v_D+\sum_{i=1}^{r} v_i \leq v$ and $q+r=\sigma$, we have

$$\begin{aligned}
\frac{h(\mathcal{G},\lambda,\lambda')\cdot 2^{qn}}{(2^n)_{|\mathcal{V}|}} &= \frac{h(\mathcal{G},\lambda,\lambda')}{(2^n-\sigma)_{|\mathcal{D}|}h(r)}\prod_{i=0}^{r-1}\frac{h(i+1)2^{n(w_{i+1}-1)}}{h(i)(2^n-\sigma_i)_{w_{i+1}}} \\
&\geq \left(1-\frac{2v_D}{2^n}\right)\prod_{i=0}^{r-1}\left(1-\frac{\sigma_i^2 w_{i+1}^2}{2^{2n}}-\frac{2v_{i+1}}{2^n}\right) \\
&\geq 1-\sum_{i=0}^{r-1}\left(\frac{\sigma_i^2 w_{i+1}^2}{2^{2n}}+\frac{2v_{i+1}}{2^n}\right)-\frac{2v_D}{2^n} \\
&\geq 1-\frac{\sigma^2}{2^{2n}}\sum_{i=1}^{r} w_i^2-\frac{2v}{2^n}. \qquad \square
\end{aligned}$$

From the definition of S and R (given in Section 2.4), (1) can be rephrased in terms of Mirror theory as follows.

Lemma 4. *For positive integers q and v, let $\mathcal{G}=(\mathcal{V},\mathcal{E}^{=}\cup\mathcal{E}^{\neq})$ be a graph such that $\mathcal{G}^{=}$ has no cycle, $|\mathcal{E}^{=}|=q$, and $\mathcal{E}^{\neq}=\emptyset$. Suppose that $\mathcal{G}^{=}$ is decomposed into its connected components as in (3). Let $w_i=|\mathcal{C}_i|$ for $i=1,\ldots,r$, and let $\sigma=\sum_{i=1}^{r} w_i$. Then we have*

$$\frac{1}{2}\sum_{\lambda\in\mathsf{Func}(\mathcal{E}^{=},\{0,1\}^n)}\left|\frac{h(\mathcal{G},\lambda)}{(2^n)_{|\mathcal{V}|}}-\frac{1}{2^{qn}}\right| \leq \left(\frac{4\sigma}{2^{2n}}\sum_{i=1}^{r} w_i^3\right)^{\frac{1}{2}}+\sum_{i=1}^{r}\frac{w_i(w_i-1)}{2^{n+1}}.$$

3 The SCM Authenticated Encryption Mode

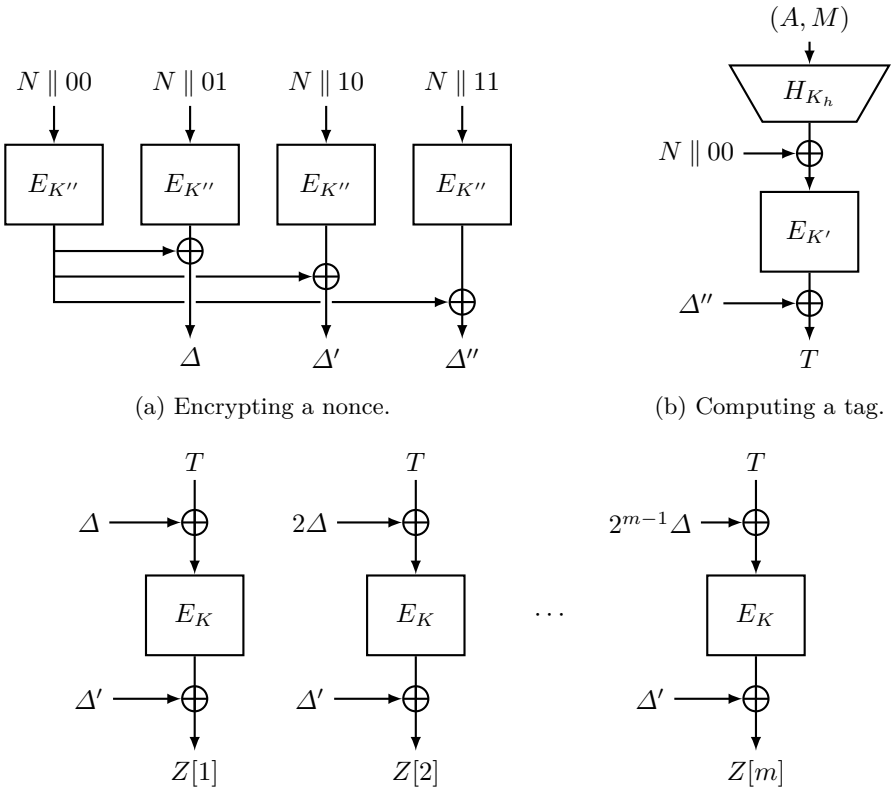
The SCM AE mode is built on top of a keyed hash function $H:\mathcal{K}_h\times(\{0,1\}^*\times\{0,1\}^*)\to\{0,1\}^n$ and a block cipher $E:\mathcal{K}_b\times\{0,1\}^n\to\{0,1\}^n$. Formally, the SCM mode based on H and E is

$$\mathsf{SCM}[H,E]=(\mathcal{K},\mathcal{N},\mathcal{A},\mathcal{M},\mathsf{SCM.ENC},\mathsf{SCM.DEC})$$

where $\mathcal{K}=\mathcal{K}_h\times\mathcal{K}_b\times\mathcal{K}_b\times\mathcal{K}_b$, $\mathcal{N}=\{0,1\}^{n-2}$, $\mathcal{A}=\mathcal{M}=\{0,1\}^*$, and SCM.ENC and SCM.DEC are deterministic algorithms. Given a key $(K_h,K,K',K'')\in\mathcal{K}$, a nonce $N\in\mathcal{N}$ and a message $M\in\mathcal{M}$ with associated data $A\in\mathcal{A}$,[6] $\mathsf{SCM}[H,E]_{K_h,K,K',K''}$ generates Δ, Δ' and Δ'', where

$$\begin{aligned}
\Delta &= E_{K''}(N\,\|\,00)\oplus E_{K''}(N\,\|\,01),\\
\Delta' &= E_{K''}(N\,\|\,00)\oplus E_{K''}(N\,\|\,10),\\
\Delta'' &= E_{K''}(N\,\|\,00)\oplus E_{K''}(N\,\|\,11).
\end{aligned}$$

[6] We assume that either $|A|>0$ or $|M|>0$.



(a) Encrypting a nonce.

(b) Computing a tag.

(c) Generating a keystream.

Fig. 3: The SCM mode based on H and E using a key (K_h, K, K', K'').

Then the tag T is defined as

$$T = E_{K'}(H_{K_h}(A, M) \oplus (N \| 00)) \oplus \Delta''.$$

Let $M = M[1] \| M[2] \| \cdots \| M[m]$ for a positive integer m, where $|M[\alpha]| = n$ for $\alpha = 1, \ldots, m-1$, and $0 < M[m] \leq n$. Then, for $\alpha = 1, \ldots, m$, the α-th keystream block $Z[\alpha]$ is defined as

$$Z[\alpha] = E_K(T \oplus 2^{\alpha-1}\Delta) \oplus \Delta',$$

where the last block is truncated so that $|Z[m]| = |M[m]|$. The keystream $Z = Z[1] \| Z[2] \| \cdots \| Z[m]$ is xored to the message M, producing the corresponding ciphertext $C = M \oplus Z$ (see Figure 3).

As shown in Figure 4, SCM.ENC and SCM.DEC can be described using the underlying MAC scheme and the PRNG, denoted SCM.MAC and SCM.PRNG, respectively.

SCM.MAC$[H, E]$

Input: $(K_h, K', K'') \in \mathcal{K}_h \times \mathcal{K}_b \times \mathcal{K}_b$, $N \in \mathcal{N}$, A, $M \in \{0,1\}^*$
Output: $T \in \{0,1\}^n$

$\Delta'' \leftarrow E_{K''}(N \,\|\, 00) \oplus E_{K''}(N \,\|\, 11)$
$X \leftarrow H_{K_h}(A, M) \oplus (N \,\|\, 00)$
$T \leftarrow E_{K'}(X) \oplus \Delta''$
return T

SCM.PRNG$[E]$

Input: $(K, K'') \in \mathcal{K}_b \times \mathcal{K}_b$, $N \in \mathcal{N}$, $T \in \{0,1\}^n$, m: nonnegative integer
Output: $Z \in \{0,1\}^*$

$\Delta \leftarrow E_{K''}(N \,\|\, 00) \oplus E_{K''}(N \,\|\, 01)$
$\Delta' \leftarrow E_{K''}(N \,\|\, 00) \oplus E_{K''}(N \,\|\, 10)$
for $i = 1, \ldots, m$ **do**
    $X[i] \leftarrow T \oplus 2^{i-1}\Delta$
    $Z[i] \leftarrow E_K(X[i]) \oplus \Delta'$
$Z \leftarrow Z[1] \,\|\, \cdots \,\|\, Z[m]$
return Z

SCM.ENC$[H, E]$

Input: $(K_h, K, K', K'') \in \mathcal{K}$, $N \in \mathcal{N}$, $A \in \mathcal{A}$, $M \in \mathcal{M}$
Output: $C \in \{0,1\}^*$, $T \in \{0,1\}^n$

$T \leftarrow \mathsf{SCM.MAC}[H, E]_{K_h, K', K''}(N, A, M)$
$m \leftarrow \lceil |M|/n \rceil$
$Z \leftarrow \mathsf{SCM.PRNG}[E]_{K, K''}(N, T, m)$
$Z \leftarrow \mathsf{msb}_{|M|}(Z)$
$C \leftarrow M \oplus Z$
return (C, T)

SCM.DEC$[H, E]$

Input: $(K_h, K, K', K'') \in \mathcal{K}$, $N \in \mathcal{N}$, $A \in \mathcal{A}$, $C \in \{0,1\}^*$, $T \in \{0,1\}^n$
Output: $M \in \mathcal{M}$ or $\perp$

$m \leftarrow \lceil |C|/n \rceil$
$Z \leftarrow \mathsf{SCM.PRNG}[E]_{K, K''}(N, T, m)$
$Z \leftarrow \mathsf{msb}_{|C|}(Z)$
$M \leftarrow C \oplus Z$
$T' \leftarrow \mathsf{SCM.MAC}[H, E]_{K_h, K', K''}(N, A, M)$
if $T \neq T'$ **then**
    return $\perp$
else
    return M

Fig. 4: Description of the SCM mode in pseudocode.

4 Security of SCM

The nAE-security of SCM is summarized by the following theorem.

Theorem 1. *Let $\delta > 0$, let $H : \mathcal{K}_h \times (\{0,1\}^* \times \{0,1\}^*) \to \{0,1\}^n$ be a δ-AXU function, and let $E : \mathcal{K}_b \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Then for nonnegative integers μ, q, v, σ, l, t such that $q + v \leq 2^{n-3}$, and for any positive integer L, we have*

$$\begin{aligned}\mathsf{Adv}^{\mathsf{nAE}}_{\mathsf{SCM}[H,E]}(\mu,q,v,\sigma,l,t) \leq\ & \min\left\{\frac{8q(\mu+1)^2l^2}{2^n}, \frac{4\sigma^3 l + 2\sigma^2\mu^2 l^2}{2^{2n}} + \frac{8\sigma l + 4\mu^2 l^2}{2^n}\right\} \\ & + \frac{16\mu^4}{2^{2n}} + \frac{\mu^2}{2^n} + 4\mu^2\delta + \frac{4v}{2^n} + (2L+1)v\delta \\ & + 2^n\left(\frac{e\mu^2}{L2^n}\right)^L + \frac{(16\sqrt{2}+6)(q+v)}{2^n} \\ & + 3\mathsf{Adv}^{\mathsf{prp}}_E(5q+5v+\sigma+vl, t+t'),\end{aligned}$$

where t' is the time complexity necessary to compute E for $5q+5v+\sigma+vl$ times.

Remark 1. When $L = n$ and $\mu \leq 2^{\frac{n}{2}}$, we have $2^n\left(\frac{e\mu^2}{L2^n}\right)^L \leq \left(\frac{2e}{n}\right)^n$, which is close to 0 for a sufficiently large n.

4.1 Proof of Theorem 1

Fix a $(\mu, q, v, \sigma, l, t)$-adversary $\mathcal{D}$ against $\mathsf{SCM}[H, E]$. Up to the prp-security of E, keyed permutations E_K, $E_{K'}$, and $E_{K''}$ can be replaced by truly random permutations π, π', and π'', respectively. Precisely, the cost of this replacement is upper bounded by

$$3\mathsf{Adv}^{\mathsf{prp}}_E(5q+5v+\sigma+vl, t+t') \tag{4}$$

since $\mathcal{D}$ makes at most $5q + 5v + \sigma + vl$ block cipher queries.

Furthermore, by Lemma 2 (with $w = 4$ and $r = q + v$ in (2)), $\pi''(\cdot \,\|\, 00) \oplus \pi''(\cdot \,\|\, 01)$, $\pi''(\cdot \,\|\, 00) \oplus \pi''(\cdot \,\|\, 10)$ and $\pi''(\cdot \,\|\, 00) \oplus \pi''(\cdot \,\|\, 11)$ (used to encrypt nonces) can be replaced by three independent random functions ρ, ρ', and ρ'', respectively, at the cost of

$$\frac{(16\sqrt{2}+6)(q+v)}{2^n}. \tag{5}$$

The resulting construction (using independent random permutations π and π', and three independent random functions ρ, ρ', and ρ'') will be denoted $\mathsf{SCM}^*[H]$.

Similarly to $\mathsf{SCM}[H, E]$, $\mathsf{SCM}^*[H]$ uses two subprocedures $\mathsf{SCM.MAC}^*[H]$ and $\mathsf{SCM.PRNG}^*$; $\mathsf{SCM.MAC}^*[H]$ takes as input a nonce $N \in \{0,1\}^{n-2}$ and a message $M \in \{0,1\}^*$ with associated data $A \in \{0,1\}^*$, and returns the tag T, where

$$T \stackrel{\text{def}}{=} \rho'(N) \oplus \pi'(H_{K_h}(A, M) \oplus (N \,\|\, 00)).$$

On the other hand, $\mathsf{SCM.PRNG}^*$ takes as input a nonce $N \in \{0,1\}^{n-2}$, a tag $T \in \{0,1\}^n$ and a nonnegative integer m such that $m \le l$, and returns a keystream $Z = Z[1] \| \cdots \| Z[m]$ and T, where

$$Z[\alpha] \stackrel{\text{def}}{=} \pi(T \oplus 2^{\alpha-1}\rho(N)) \oplus \rho'(N)$$

for $\alpha = 1, \ldots, m$.

For our security proof, we consider a slightly modified variant of $\mathsf{SCM.PRNG}^*$, denoted $\mathsf{SCM.PRNG}^{\#}$, that takes as input a nonce $N \in \{0,1\}^{n-2}$ and a nonnegative integer m such that $m \le l$, and returns $\mathsf{SCM.PRNG}^*_{\pi,\rho,\rho'}(N,T,m)$ and T, where T is chosen uniformly at random from $\{0,1\}^n$. For an adversary $\mathcal{B}$ making oracle queries to $\mathsf{SCM.PRNG}^{\#}$, its distinguishing advantage is defined as

$$\mathsf{Adv}^{\mathsf{prg}}_{\mathsf{SCM.PRNG}^{\#}}(\mathcal{B}) \stackrel{\text{def}}{=} \left|\Pr\left[\mathcal{B}^{\mathsf{SCM.PRNG}^{\#}} = 1\right] - \Pr\left[\mathcal{B}^{\$} = 1\right]\right|$$

where the ideal oracle \$ takes as input N and m, and returns a tuple of a random nm-bit string and a random n-bit string. Note that \$ is a sampling that returns a fresh random value for every redundant query.[7]

A (μ, q, σ, l)-adversary against $\mathsf{SCM.PRNG}^{\#}$ is an (information-theoretic) algorithm that makes at most q queries with at most μ faulty queries (using repeated nonces), where $m \le l$ for every query, and the sum of m over all the queries is at most σ. Then we define $\mathsf{Adv}^{\mathsf{prg}}_{\mathsf{SCM.PRNG}^{\#}}(\mu, q, \sigma, l)$ as the maximum of $\mathsf{Adv}^{\mathsf{prg}}_{\mathsf{SCM.PRNG}^{\#}}(\mathcal{B})$ over all (μ, q, σ, l)-adversaries $\mathcal{B}$ against $\mathsf{SCM.PRNG}^{\#}$. With this notion of security, we can prove the following lemma.

Lemma 5. *Let $\delta > 0$, let $H : \mathcal{K}_h \times (\{0,1\}^* \times \{0,1\}^*) \mapsto \{0,1\}^n$ be a δ-AXU function. Then for nonnegative integers μ, q, v, σ, l, we have*

$$\mathsf{Adv}^{\mathsf{nAE}}_{\mathsf{SCM}^*[H]}(\mu, q, v, \sigma, l) \le \mathsf{Adv}^{\mathsf{mac}}_{\mathsf{SCM.MAC}^*[H]}(\mu, q, v) + \mathsf{Adv}^{\mathsf{prg}}_{\mathsf{SCM.PRNG}^{\#}}(\mu, q, \sigma, l)$$

The MAC security of $\mathsf{SCM.MAC}^*[H]$ is proved as follows.

Lemma 6. *Let $\delta > 0$, and let $H : \mathcal{K} \times (\{0,1\}^* \times \{0,1\}^*) \mapsto \{0,1\}^n$ be a δ-AXU hash function. For nonnegative integers μ, q, v, such that $q + v \le 2^{n-3}$ and for any positive integer L, we have*

$$\mathsf{Adv}^{\mathsf{mac}}_{\mathsf{SCM.MAC}^*[H]}(\mu, q, v) \le \frac{16\mu^4}{2^{2n}} + \frac{\mu^2}{2^n} + 4\mu^2\delta + \frac{4v}{2^n} + (2L+1)v\delta + 2^n\left(\frac{e\mu^2}{L2^n}\right)^L.$$

The following lemmas upper bound the adversarial distinguishing advantage against $\mathsf{SCM.PRNG}^{\#}$ using two different approaches.

Lemma 7. *For nonnegative integers μ, q, σ, and l, we have*

$$\mathsf{Adv}^{\mathsf{prg}}_{\mathsf{SCM.PRNG}^{\#}}(\mu, q, \sigma, l) \le \frac{4\sigma^3 l + 2\sigma^2\mu^2 l^2}{2^{2n}} + \frac{8\sigma l + 4\mu^2 l^2}{2^n}.$$

[7] This property might allow an adversary to distinguish $\mathsf{SCM.PRNG}^{\#}$ and \$ by making redundant queries, and this aspect will be taken into account in Lemma 7 and 8.

Lemma 8. *For nonnegative integers μ, q, σ, and l, we have*

$$\mathsf{Adv}^{\mathsf{prg}}_{\mathsf{SCM.PRNG}^{\#}}(\mu, q, \sigma, l) \le \frac{8q(\mu+1)^2 l^2}{2^n}.$$

The proof of Theorem 1 is complete by (4), (5), Lemma 5, 6, 7 and 8.

4.2 Proof of Lemma 5

For three types of arbitrary functions

$$\begin{aligned} \mathsf{Auth} &: \mathcal{N} \times \mathcal{A} \times \mathcal{M} \mapsto \{0,1\}^n, \\ \mathsf{Ver} &: \mathcal{N} \times \mathcal{A} \times \mathcal{M} \times \{0,1\}^n \mapsto \{\top, \bot\}, \\ \mathsf{G} &: \mathcal{N} \times \{0,1\}^n \times \{0,\ldots,l\} \mapsto \{0,1\}^* \end{aligned}$$

such that $|\mathsf{G}(\cdot,\cdot,m)| = nm$, we define combiners, Enc for Auth and G, and Dec for Ver and G, where

- for $N \in \mathcal{N}$, $A \in \mathcal{A}$, $M \in \mathcal{M}$,

$$\mathsf{Enc}[\mathsf{Auth}, \mathsf{G}](N, A, M) = (M \oplus \mathsf{msb}_{|M|}(\mathsf{G}(N, T, m)), T)$$

  where $T = \mathsf{Auth}(N, A, M)$ and $m = \lceil |M|/n \rceil$;
- for $N \in \mathcal{N}$, $A \in \mathcal{A}$, $C \in \{0,1\}^*$ and $T \in \{0,1\}^n$,

$$\mathsf{Dec}[\mathsf{Ver}, \mathsf{G}](N, A, C, T) = \begin{cases} M & \text{if } \mathsf{Ver}(N, A, M, T) = \top \\ \bot & \text{if } \mathsf{Ver}(N, A, M, T) = \bot \end{cases}$$

  where $M = C \oplus \mathsf{msb}_{|C|}(\mathsf{G}(N, T, m))$ and $m = \lceil |C|/n \rceil$.

Let Auth^* and Ver^* denote the MAC and the verification oracle of $\mathsf{SCM.MAC}^*[H]$, respectively. Then, $\mathsf{Enc}[\mathsf{Auth}^*, \mathsf{SCM.PRNG}^*]$ and $\mathsf{Dec}[\mathsf{Ver}^*, \mathsf{SCM.PRNG}^*]$ become the encryption and the decryption oracle of $\mathsf{SCM}^*[H]$, respectively.[8] We define three worlds World_i, $i = 1, 2, 3$, as follows.

$$\begin{aligned} \mathsf{World}_1 &\stackrel{\text{def}}{=} (\mathsf{Enc}[\mathsf{Auth}^*, \mathsf{SCM.PRNG}^*], \mathsf{Dec}[\mathsf{Ver}^*, \mathsf{SCM.PRNG}^*]), \\ \mathsf{World}_2 &\stackrel{\text{def}}{=} (\mathsf{Enc}[\mathsf{R}, \mathsf{SCM.PRNG}^*], \mathsf{Dec}[\mathsf{Rej}, \mathsf{SCM.PRNG}^*]), \\ \mathsf{World}_3 &\stackrel{\text{def}}{=} (\mathsf{Rand}, \mathsf{Rej}), \end{aligned}$$

where R is a random n-bit function, Rej always returns $\bot$, and Rand returns a pair of a random string of $|M|$ bits and a random string of n bits, being independent of each other, when it takes as input $(N, A, M) \in \mathcal{N} \times \mathcal{A} \times \mathcal{M}$. Then, for a

[8] For simplicity of notation, we write $\mathsf{SCM.PRNG}^*$ to denote $\mathsf{SCM.PRNG}^*_{\pi,\rho,\rho'}$ for a random permutation π, and random functions ρ and ρ'.

(μ, q, v, σ, l)-adversary $\mathcal{D}$ against the nonce-based AE security of $\mathsf{SCM}^*[H]$, we have

$$\begin{aligned}\mathsf{Adv}^{\mathsf{nAE}}_{\mathsf{SCM}^*}(\mathcal{D}) &= \left|\Pr\left[\mathcal{D}^{\mathsf{World}_1}=1\right]-\Pr\left[\mathcal{D}^{\mathsf{World}_3}=1\right]\right| \\ &\le \left|\Pr\left[\mathcal{D}^{\mathsf{World}_1}=1\right]-\Pr\left[\mathcal{D}^{\mathsf{World}_2}=1\right]\right| \\ &\quad + \left|\Pr\left[\mathcal{D}^{\mathsf{World}_2}=1\right]-\Pr\left[\mathcal{D}^{\mathsf{World}_3}=1\right]\right|. \end{aligned} \tag{6}$$

Since World_1 and World_2 use $(\mathsf{Auth}^*, \mathsf{Ver}^*)$ and $(\mathsf{R}, \mathsf{Rej})$ as their subprocedures, we have

$$\left|\Pr\left[\mathcal{D}^{\mathsf{World}_1}=1\right]-\Pr\left[\mathcal{D}^{\mathsf{World}_2}=1\right]\right| \le \mathsf{Adv}^{\mathsf{mac}}_{\mathsf{SCM.MAC}^*}(\mu, q, v). \tag{7}$$

In both World_2 and World_3, the second oracle behaves in the same way, always returning $\perp$. So without loss of generality, we can assume that $\mathcal{D}$ makes queries only to the first oracle. Then we can construct an adversary $\mathcal{D}'$ against the pseudorandomness of $\mathsf{SCM.PRNG}^{\#}$ by using $\mathcal{D}$ as a subroutine, and faithfully simulating World_2 and World_3 using oracles $\mathsf{SCM.PRNG}^{\#}$ and Rand, respectively; given an oracle $\mathcal{O} \in \{\mathsf{SCM.PRNG}^{\#}, \$\}$, $\mathcal{D}$'s query with (N, A, M) is answered with $(M \oplus \mathsf{msb}_{|M|}(Z), T)$, where $(Z, T) = \mathcal{O}(N, m)$ for $m = \lceil |M|/n \rceil$. Assuming that $\mathcal{D}$ makes no redundant query without loss of generality, we have

$$\left|\Pr\left[\mathcal{D}^{\mathsf{World}_2}=1\right]-\Pr\left[\mathcal{D}^{\mathsf{World}_3}=1\right]\right| \le \mathsf{Adv}^{\mathsf{prg}}_{\mathsf{SCM.PRNG}^{\#}}(\mu, q, \sigma, l). \tag{8}$$

By (6), (7) and (8), we have

$$\mathsf{Adv}^{\mathsf{nAE}}_{\mathsf{SCM}^*}(\mu, q, v, \sigma, l) \le \mathsf{Adv}^{\mathsf{mac}}_{\mathsf{SCM.MAC}^*}(\mu, q, v) + \mathsf{Adv}^{\mathsf{prg}}_{\mathsf{SCM.PRNG}^{\#}}(\mu, q, \sigma, l).$$

4.3 Proof of Lemma 6

Suppose that an adversary $\mathcal{A}$ makes q authentication queries using at most μ faulty nonces, and makes v verification queries, where $q + v \le 2^{n-3}$. Let

$$\begin{aligned}\tau_m &= (N_i, (A_i, M_i), T_i)_{1 \le i \le q}\,, \\ \tau_v &= \left(N'_j, (A'_j, M'_j), T'_j, b'_j\right)_{1 \le j \le v}\end{aligned}$$

denote the list of authentication queries and verification queries, respectively. At the end of the interaction, we will give K_h to $\mathcal{A}$ for free. In the ideal world, a dummy key K_h will be selected uniformly at random from $\mathcal{K}$, and given to $\mathcal{A}$. Then, from the transcript

$$\tau = (K_h, \tau_m, \tau_v)\,,$$

one can fix $X_i = H_{K_h}(A_i, M_i) \oplus (N_i \,\|\, 00)$ for $i \in [q]$, and $X'_j = H_{K_h}(A'_j, M'_j) \oplus (N'_j \,\|\, 00)$ for $j \in [v]$. A transcript $\tau = (K_h, \tau_m, \tau_v)$ is defined as *bad* if one of the following conditions holds.

- $\mathsf{bad}_1 \Leftrightarrow$ there exists $(i, j) \in [q]^{*2}$ such that $N_i = N_k$ for some $k(\neq i)$, $N_j = N_l$ for some $l(\neq j)$ and $X_i = X_j$;

– $\mathsf{bad}_2 \Leftrightarrow$ there exists $(i,j) \in [q]^{*2}$ such that $N_i = N_j$ and $T_i = T_j$;
– $\mathsf{bad}_3 \Leftrightarrow$ there exists $i \in [q]$ and $j \in [v]$ such that $N_i = N'_j$, $X_i = X'_j$, and $T_i = T'_j$;
– $\mathsf{bad}_4 \Leftrightarrow$ there exists $(i,j,k) \in [q]^{*3}$ and $l \in [v]$ such that $X_i = X_j$, $N_j = N_k$, $X_k = X'_l$, $N'_l = N_i$ and $T_i \oplus T_j \oplus T_k \oplus T'_l = \mathbf{0}$.

If a transcript τ is not bad, then it will be called a *good* transcript. The probability of obtaining a bad transcript in the ideal world is upper bounded as follows.

Lemma 9. *For any positive integer L, we have*

$$\Pr[\mathsf{T}_{\mathsf{id}} \in \mathit{\Gamma}_{\mathsf{bad}}] \le \frac{\mu^2}{2^n} + 4\mu^2\delta + \frac{v}{2^n} + (2L+1)v\delta + 2^n \left(\frac{e\mu^2}{L2^n}\right)^L.$$

Proof. We fix a positive number L. Let

$$I_T \stackrel{\text{def}}{=} \{i \in [q] : N_i = N_j \text{ and } T_i \oplus T_j = T \text{ for some } j \text{ such that } j < i\}$$

for $T \in \{0,1\}^n$, and then define the following auxiliary event.

– $\mathsf{aux} \Leftrightarrow$ there exists $T^* \in \{0,1\}^n$ such that $|I_{T^*}| > L$.

1. For fixed $T \in \{0,1\}^n$ and $i \in [q]$, suppose that $i \in I_T$. It means that the i-th query is faulty, and that $T_i \oplus T_j = T$ for any (previous) j-th query such that $N_i = N_j$, which happens with probability at most $\mu/2^n$. Therefore we have

$$\Pr[\mathsf{aux}] \le 2^n \binom{\mu}{L} \left(\frac{\mu}{2^n}\right)^L \le 2^n \left(\frac{e\mu^2}{L2^n}\right)^L.$$

2. The number of queries using any repeated nonce is at most 2μ. So the number of pairs $(i,j) \in [q]^{*2}$ such that $N_i = N_k$ for some $k(\neq i)$ and $N_j = N_l$ for some $l(\neq j)$ is at most $4\mu^2$. For each of such pairs, say (i,j), the probability that $X_i = X_j$ is at most δ. Therefore, we have

$$\Pr[\mathsf{bad}_1] \le 4\mu^2\delta.$$

3. By symmetry, we can assume that $i < j$, which means that N_j is a faulty nonce. For each MAC query using a faulty nonce, there are at most μ other queries using the same nonce. So the number of pairs (i,j) such that $i < j$ and $N_i = N_j$ is at most μ^2. For each of such pairs (i,j), the probability that $T_i = T_j$ is $\frac{1}{2^n}$. Therefore, we have

$$\Pr[\mathsf{bad}_2] \le \frac{\mu^2}{2^n}.$$

4. (a) For each verification query (N'_j, M'_j, T'_j), there is at most one MAC query (N_i, M_i, T_i) such that $N_i = N'_j$ and $M_i = M'_j$. For this pair of indices, the probability that $T_i = T'_j$ is upper bounded by $\frac{1}{2^n}$.

(b) For each verification query (N'_j, M'_j, T'_j), there is at most one MAC query (N_i, M_i, T_i) such that $N_i = N'_j$, $M_i \neq M'_j$ and $T_i = T'_j$ without bad_2, since otherwise there would be a pair of MAC queries whose nonces and tags are all the same. For this pair of indices, the probability that $X_i = X'_j$ is upper bounded by δ.

Therefore, we have

$$\Pr[\mathsf{bad}_3 \mid \neg\mathsf{bad}_2] \leq v\delta + \frac{v}{2^n}.$$

5. Fix a verification query index $l \in [v]$. If there are two distinct MAC queries, say (N_i, M_i, T_i) and $(N_{i'}, M_{i'}, T_{i'})$, such that $N_i = N_{i'} = N'_l$, then the l-th verification query cannot contribute to bad_4 without making bad_1. So we can assume that there is a single MAC query, say (N_i, M_i, T_i), such that $N_i = N'_l$. Let $T = T_i \oplus T'_l$. In order for the l-th verification query to contribute to bad_4, it should be the case that either $X_i = X_j$ for some $j \in I_T$ such that $j \neq i$ or $X'_l = X_j$ for some $j \in I_T$ such that $N_j \neq N'_l$, where $|I_T| \leq L$ without aux. Overall, we have

$$\Pr\left[\mathsf{bad}_4 \wedge \neg\mathsf{bad}_1 \wedge \neg\mathsf{aux}\right] \leq 2Lv\delta.$$

Therefore, we have

$$\begin{aligned}
\Pr[\mathsf{T}_{\mathsf{id}} \in \mathit{\Gamma}_{\mathsf{bad}}] &\leq \Pr[\mathsf{aux} \vee \mathsf{bad}_1 \vee \mathsf{bad}_2 \vee \mathsf{bad}_3 \vee \mathsf{bad}_4] \\
&\leq \Pr[\mathsf{aux}] + \Pr[\mathsf{bad}_1] + \Pr[\mathsf{bad}_2] + \Pr[\mathsf{bad}_3 \mid \neg\mathsf{bad}_2] \\
&\quad + \Pr\left[\mathsf{bad}_4 \wedge \neg\mathsf{bad}_1 \wedge \neg\mathsf{aux}\right] \\
&\leq \frac{\mu^2}{2^n} + 4\mu^2\delta + \frac{v}{2^n} + (2L+1)v\delta + 2^n\left(\frac{e\mu^2}{L2^n}\right)^L. \qquad \square
\end{aligned}$$

Fix a good transcript $\tau = (K_h, \tau_m, \tau_v)$. Let

$$\mathcal{V} = \{\pi'(X_1), \ldots, \pi'(X_q)\} \cup \{\pi'(X'_1), \ldots, \pi'(X'_v)\}$$

where the elements of $\mathcal{V}$ can be viewed as unknowns (to be determined by a random permutation π'). We will define a graph $\mathcal{G}_\tau = (\mathcal{V}, \mathcal{E}^{=} \sqcup \mathcal{E}^{\neq})$, and label functions $\lambda : \mathcal{E}^{=} \to \{0,1\}^n$ and $\lambda' : \mathcal{E}^{\neq} \to \{0,1\}^n$ as follows.

- Let $\mathcal{N}_m = \{N_1, \ldots, N_q\}$ and let $\mathcal{N}_v = \{N'_1, \ldots, N'_v\}$. They are not necessarily disjoint.
- For each nonce $N \in \mathcal{N}_m$, let $P_N \in \mathcal{V}$ denote the vertex corresponding to $\pi'(X_i)$, where $i \in [q]$ is the *smallest* index such that $N_i = N$. Any vertex $\pi'(X_j)$ such that $N_j = N$ and $j > i$ is connected with P_N by an $=$-labeled edge; for such an edge, we define

$$\lambda(\pi'(X_i), \pi'(X_j)) \stackrel{\text{def}}{=} T_i \oplus T_j.$$

The resulting graph that consists of P_N and their neighbors will be denoted $\mathcal{C}^{=}_N$. We note the following properties.

- There is no loop at P_N since otherwise we have $(i,j) \in [q]^{*2}$ such that $N_i = N_j$ and $X_i = X_j$, implying bad_1. So, for any $N \in \mathcal{N}_m$, $\mathcal{C}^{=}_N$ is a tree.
- For distinct N_i and N_j in $\mathcal{N}_m$ such that $|\mathcal{C}^{=}_{N_i}|, |\mathcal{C}^{=}_{N_j}| \geq 2$, $\mathcal{C}^{=}_{N_i}$ and $\mathcal{C}^{=}_{N_j}$ are disjoint since otherwise we have bad_1 around the i-th and the j-th queries.

– Let

$$\mathcal{G}^{=}_{\tau} \stackrel{\text{def}}{=} \bigsqcup_{\substack{N \in \mathcal{N}_m \\ \text{such that } |\mathcal{C}^{=}_N| \geq 2}} \mathcal{C}^{=}_N \sqcup \mathcal{V}^*,$$

where $\mathcal{V}^*$ denotes the set of isolated vertices of $\mathcal{V}$.

– For any $N \in \mathcal{N}_m \cap \mathcal{N}_v$, suppose that $P_N = \pi'(X_i)$ and $N = N'_j$ for some $i \in [q]$ and $j \in [v]$, $\pi'(X_i)$. Then $\pi'(X_i)$ and $\pi'(X'_j)$ are connected by a $\neq$-labeled edge, where

$$\lambda'(\pi'(X_i), \pi'(X'_j)) \stackrel{\text{def}}{=} T_i \oplus T'_j.$$

– Finally, $\mathcal{G}_{\tau}$ is obtained from $\mathcal{G}^{=}_{\tau}$ by adding all the $\neq$-labeled edges.

We note the following properties.

1. $\mathcal{G}^{=}_{\tau}$ does not contain a trail of length more than two.
2. For any two vertices $\pi'(X_i)$ and $\pi'(X_j)$ in the same component $\mathcal{C}^{=}_{N_i} (= \mathcal{C}^{=}_{N_j})$,

$$\bar{\lambda}(\pi'(X_i), \pi'(X_j)) = T_i \oplus T_j \neq \mathbf{0},$$

since otherwise we have bad_2.

3. If two vertices $\pi'(X_i)$ and $\pi'(X_j)$, not necessarily distinct, are connected by a $\neq$-labeled edge in the same component in $\mathcal{G}^{=}_{\tau}$, and if $\pi'(X_j) = \pi'(X'_k)$ and $\pi'(X_i) = \pi'(X_l)$ for some $k \in [v]$ and $l \in [q]$ such that $N_l = N'_k$, then

$$\bar{\lambda}(\pi'(X_i), \pi'(X_j)) = T_i \oplus T_j \neq T_l \oplus T'_k = \lambda'(\pi'(X_l), \pi'(X'_k)),$$

since otherwise we have either bad_3 (when $i = l$) or bad_4 (when $i \neq l$).

Due to the above properties, we can apply Lemma 3 to $\mathcal{G}_{\tau}$. More precisely, we will lower bound the probability of obtaining the good transcript τ in the real world by the following steps.

1. The number of possible assignments of distinct values to the vertices of $\mathcal{G}_{\tau}$ is lower bounded by

$$\frac{(2^n)_{|\mathcal{V}|}}{2^{|\mathcal{E}^{=}|n}} \left(1 - \frac{16\mu^4}{2^{2n}} - \frac{2v}{2^n}\right)$$

by Lemma 3, where $|\mathcal{E}^{\neq}| \leq v$, $\sigma \leq 2|\mathcal{E}^{=}| \leq 2\mu$ and $\sum_{i=1}^{r} w_i^2 \leq 4\mu^2$, since $\sum_{i=1}^{r} w_i^2 \leq \sigma^2 \leq 4|\mathcal{E}^{=}|^2$ and $|\mathcal{E}^{=}|$ is the number of faulty queries in τ such that $|\mathcal{E}^{=}| \leq \mu$. The probability that a random permutation π' realizes each assignment is $1/(2^n)_{|\mathcal{V}|}$.

2. The above assignment uniquely determines $\rho''(N)$ for any $N \in \mathcal{N}_m \cap \mathcal{N}_v$ without any contradiction.
3. For each $N \in \mathcal{N}_v \setminus \mathcal{N}_m$, the number of possible values for $\rho''(N)$ is at least $2^n - v_N$, where v_N denotes the number of verification queries using nonce N.
4. Once the assignment of values to $\rho''(N)$, $N \in \mathcal{N}_m \cup \mathcal{N}_v$, is fixed, then the probability that a random function ρ'' realizes this assignment is given as $1/(2^n)^{|\mathcal{N}_m \cup \mathcal{N}_v|}$.

Since $\Pr[\mathsf{T}_{\mathsf{id}} = \tau] = \frac{1}{2^{qn}}$, $\sum_{N \in \mathcal{N}_v \setminus \mathcal{N}_m} v_N \le v$, and

$$|\mathcal{N}_m \cup \mathcal{N}_v| = |\mathcal{N}_v \setminus \mathcal{N}_m| + |\mathcal{N}_m| = |\mathcal{N}_v \setminus \mathcal{N}_m| + q - |\mathcal{E}^{=}|,$$

we have

$$\begin{aligned}
\frac{\Pr[\mathsf{T}_{\mathsf{re}} = \tau]}{\Pr[\mathsf{T}_{\mathsf{id}} = \tau]} &\ge \frac{1}{2^{|\mathcal{E}^{=}|n}} \left(1 - \frac{16\mu^4}{2^{2n}} - \frac{2v}{2^n}\right) \cdot \left(\prod_{N \in \mathcal{N}_v \setminus \mathcal{N}_m} (2^n - v_N)\right) \cdot \frac{2^{qn}}{(2^n)^{|\mathcal{N}_m \cup \mathcal{N}_v|}} \\
&\ge \frac{1}{2^{|\mathcal{E}^{=}|n}} \left(1 - \frac{16\mu^4}{2^{2n}} - \frac{2v}{2^n}\right) \cdot \left(\prod_{N \in \mathcal{N}_v \setminus \mathcal{N}_m} \left(1 - \frac{v_N}{2^n}\right)\right) \cdot \frac{(2^n)^{|\mathcal{N}_v \setminus \mathcal{N}_m| + q}}{(2^n)^{|\mathcal{N}_m \cup \mathcal{N}_v|}} \\
&\ge 1 - \frac{16\mu^4}{2^{2n}} - \frac{3v}{2^n}. \qquad (9)
\end{aligned}$$

By Lemma 1 and 9, and (9), we completes the proof of Lemma 6.

4.4 Proof of Lemma 7

Let $\mathcal{D}$ be a (μ, q, σ, l)-adversary against the pseudorandomness of $\mathsf{SCM.PRNG}^{\#}$, assuming that $\mathcal{D}$ makes exactly q encryption queries without loss of generality. At the end of the interaction, $\mathcal{D}$ will be given $\Delta_i =^{\mathrm{def}} \rho(N_i)$, $i = 1, \ldots, q$, for free. In the ideal world, dummy masks Δ_i will be defined by an independent random function $\rho : \mathcal{N} \to \{0,1\}^n$, and given to $\mathcal{D}$. Then the transcript is defined as

$$\tau \stackrel{\mathrm{def}}{=} (N_i, m_i, \Delta_i, T_i, Z_i[1] \,\|\, \cdots \,\|\, Z_i[m_i])_{i \in [q]}.$$

From this transcript, one can fix $X_i = X_i[1] \,\|\, \cdots \,\|\, X_i[m_i]$, where

$$X_i[\alpha] \stackrel{\mathrm{def}}{=} T_i \oplus 2^{\alpha - 1} \Delta_i$$

for $i \in [q]$ and $\alpha \in [m_i]$. Let

$$\begin{aligned}
\mathcal{N}_m &= \{N_1, \ldots, N_q\}, \\
\mathcal{V} &= \{\pi(X_i[\alpha]) : i \in [q], \alpha \in [m_i]\}.
\end{aligned}$$

For $N \in \mathcal{N}_m$, let

$$\mathcal{V}_N \stackrel{\mathrm{def}}{=} \{\pi(X_i[\alpha]) : N_i = N, i \in [q], \alpha \in [m_i]\}.$$

For simplicity of notation, we rename the elements of $\mathcal{V}_N$, writing

$$\mathcal{V}_N = \{V_N[1], \ldots, V_N[s_N]\},$$

where s_N is the sum of m_i over all $i \in [q]$ such that $N_i = N$. The following bound will be useful in our security proof.

Property 1. $\sum_{N \in \mathcal{N}_m} s_N^2 \leq 2\sigma l + \mu^2 l^2$.

Proof. Let $\mathcal{F}$ denote the index set of faulty queries, namely,

$$\mathcal{F} = \{i \in [q] : N_i = N_j \text{ for some } j \text{ such that } j < i\}.$$

Since $\sum_{i \in [q] \setminus \mathcal{F}} (s_{N_i} - m_i) \leq \mu l$, we have

$$\begin{aligned} \sum_{N \in \mathcal{N}_m} s_N^2 &= \sum_{i \in [q] \setminus \mathcal{F}} (m_i + (s_{N_i} - m_i))^2 \\ &\leq \sum_{i \in [q] \setminus \mathcal{F}} \left(2m_i s_{N_i} + (s_{N_i} - m_i)^2\right) \leq 2\sigma l + \mu^2 l^2. \end{aligned}$$

□

For $V_N[\alpha] \in \mathcal{V}_N$ such that $V_N[\alpha] = \pi(X_i[\beta])$, let $W_N[\alpha]$ denote the corresponding keysteam block $Z_i[\beta]$. This means that $W_N[\alpha] = V_N[\alpha] \oplus \rho'(N)$. A transcript τ is defined as *bad* if one of the following conditions holds.

- $\mathsf{bad}_1 \Leftrightarrow \bigvee_{t \geq 1} \mathsf{bad}_1[t]$, where $\mathsf{bad}_1[t]$ if and only if there exist $(N[i])_{i \in [t]} \in \mathcal{N}_m^{*t}$, $(\alpha_i)_{i \in [t]}$ and $(\beta_i)_{i \in [t]}$ such that $\alpha_i \neq \beta_i$ and

  $$V_{N[i]}[\beta_i] = V_{N[i+1]}[\alpha_{i+1}]$$

  for $i = 1, \ldots, t$, with indices taken modulo t;
- $\mathsf{bad}_2 \Leftrightarrow \bigvee_{t \geq 1} \mathsf{bad}_2[t]$, where $\mathsf{bad}_2[t]$ if and only if there exist $(N[i])_{i \in [t]} \in \mathcal{N}_m^{*t}$, $(\alpha_i)_{i \in [t]}$ and $(\beta_i)_{i \in [t]}$ such that $\alpha_i \neq \beta_i$ and

  $$V_{N[i]}[\beta_i] = V_{N[i+1]}[\alpha_{i+1}]$$

  for $i = 1, \ldots, t-1$, and

  $$\sum_{i=1}^{t} \left(W_{N[i]}[\beta_i] \oplus W_{N[i]}[\alpha_i]\right) = \mathbf{0}.$$

The probability of each bad event (in the ideal world) is upper bounded as follows.

Lemma 10. $\Pr[\mathsf{bad}_1 \vee \mathsf{bad}_2] \leq \frac{8\sigma l + 4\mu^2 l^2}{2^n}$.

Sketch of Proof. For a fixed $t \geq 1$, consider $(N[i])_{i \in [t]} \in \mathcal{N}_m^{*t}$, $(\alpha_i)_{i \in [t]}$ and $(\beta_i)_{i \in [t]}$. The number of possibilities for such sequences is upper bounded by $\left(\sum_{N \in \mathcal{N}_m} s_N^2\right)^t$. Suppose that $V_{N[i]}[\beta_i]$ and $V_{N[i+1]}[\alpha_{i+1}]$ are defined by the γ-th

block of the j-th query and the δ-th block of the k-th query, respectively. Then the equation $V_{N[i]}[\beta_i] = V_{N[i+1]}[\alpha_{i+1}]$ is equivalent to

$$T_j \oplus 2^{\gamma-1}\Delta_j = T_k \oplus 2^{\delta-1}\Delta_k.$$

In this way, $\mathsf{bad}_1[t]$ defines t equations, where we focus on $t+1$ random variables, namely, all the Δ-values and the T-value for the last query (with the other T-values fixed). From the $2^{(t+1)n}$ possible values for these variables, one can always find out 2^n solutions to this system of equations. Therefore, the system of equations holds with probability $\frac{1}{2^{tn}}$. Then, by Property 1, we have

$$\Pr\left[\mathsf{bad}_1\right] \leq \sum_{t=1}^{\infty} \Pr\left[\mathsf{bad}_1[t]\right] \leq \sum_{t=1}^{\infty} \frac{\left(2\sigma l + \mu^2 l^2\right)^t}{2^{tn}},$$

and hence, $\Pr\left[\mathsf{bad}_1\right] \leq \frac{4\sigma l + 2\mu^2 l^2}{2^n}$ since

$$\sum_{t=1}^{\infty} \left(\frac{2\sigma l + \mu^2 l^2}{2^n}\right)^t \leq \frac{4\sigma l + 2\mu^2 l^2}{2^n}$$

if $\frac{2\sigma l + \mu^2 l^2}{2^n} \leq \frac{1}{2}$, and $\frac{4\sigma l + 2\mu^2 l^2}{2^n} > 1$ otherwise. With a similar argument to the analysis of bad_1, we can also prove that $\Pr\left[\mathsf{bad}_2\right] \leq \frac{4\sigma l + 2\mu^2 l^2}{2^n}$, which completes the proof. □

If a transcript is not bad, then it will be called a *good* transcript. For a good transcript τ, we make some noteworthy observations as follows.

1. Distinct pairs $(i, \alpha) \in [q] \times [m_i]$ and $(j, \beta) \in [q] \times [m_j]$ such that $N_i = N_j$ correspond to distinct elements of $\mathcal{V}_{N_i} (= \mathcal{V}_{N_j})$ since otherwise we have $\mathsf{bad}_1[1]$. Therefore, we have $|\mathcal{V}_N| = s_N$ for any $N \in \mathcal{N}_m$.
2. For any pair of distinct nonces N and N', $|\mathcal{V}_N \cap \mathcal{V}_{N'}| \leq 1$ since otherwise we have $\mathsf{bad}_1[1] \vee \mathsf{bad}_1[2]$.
3. Assuming $\neg(\mathsf{bad}_1[1] \vee \mathsf{bad}_1[2])$, for each nonce $N \in \mathcal{N}_m$, we can define a tree $\mathcal{T}_N = (\mathcal{V}_N, \mathcal{E}_N^{=})$, and a label function λ_N on $\mathcal{E}_N^{=}$, where any vertex $V_N[\alpha]$ such that $\alpha \geq 2$ is connected with $V_N[1]$, and

$$\lambda_N(V_N[1], V_N[\alpha]) \stackrel{\text{def}}{=} W_N[1] \oplus W_N[\alpha].$$

   We define a graph $\mathcal{G}_\tau = (\mathcal{V}, \mathcal{E}^{=})$ and a label function $\lambda : \mathcal{E}^{=} \to \{0,1\}^n$ as the union of $\mathcal{T}_N$ and the union of λ_N over all nonces in $\mathcal{N}_m$, respectively. Then,
   (a) there is no cycle in $\mathcal{G}_\tau$ since otherwise we have bad_1;
   (b) there is no pair of two vertices P and Q such that $\bar{\lambda}(P, Q) = \mathbf{0}$ since otherwise have bad_2.

Due to the above properties, we can apply Lemma 3 to $\mathcal{G}_\tau$ when τ is a good transcript. Let $\mathsf{Comp}(\mathcal{G}_\tau)$ denote the set of connected components of $\mathcal{G}_\tau$. We will lower bound the probability of obtaining the good transcript τ in the real world by the following steps.

1. Since the number of distinct nonces used in τ is $|\mathcal{N}_m|$, the probability that a random function ρ realizes (Δ_i) is $\frac{1}{2^{|\mathcal{N}_m|n}}$.
2. The probability that a random sampling realizes (T_i) is $\frac{1}{2^{qn}}$.
3. The number of possible assignments of distinct values to the vertices of $\mathcal{G}_\tau$ is lower bounded by

$$\frac{(2^n)_{|\mathcal{V}|}}{2^{|\mathcal{E}^=|n}}\left(1-\frac{\sigma^2}{2^{2n}}\sum_{\mathcal{C}\in\mathsf{Comp}(\mathcal{G}_\tau)}|\mathcal{C}|^2\right)$$

   by Lemma 3 with $|\mathcal{E}^{\neq}|=0$. The probability that a random permutation π realizes each assignment is $1/(2^n)_{|\mathcal{V}|}$.
4. The above assignment uniquely determines $\rho'(N)$ for any $N\in\mathcal{N}_m$ (without any contradiction), and the probability that a random function ρ' realizes each assignment is $\frac{1}{2^{|\mathcal{N}_m|n}}$.

Therefore, we have

$$\Pr\left[\mathsf{T}_{\mathsf{re}}=\tau\right]\geq\frac{1}{2^{(q+2|\mathcal{N}_m|+|\mathcal{E}^=|)n}}\left(1-\frac{\sigma^2}{2^{2n}}\sum_{\mathcal{C}\in\mathsf{Comp}(\mathcal{G}_\tau)}|\mathcal{C}|^2\right).$$

Since $\Pr\left[\mathsf{T}_{\mathsf{id}}=\tau\right]=\frac{1}{2^{(q+2|\mathcal{N}_m|+|\mathcal{E}^=|)n}}$, we have

$$\frac{\Pr\left[\mathsf{T}_{\mathsf{re}}=\tau\right]}{\Pr\left[\mathsf{T}_{\mathsf{id}}=\tau\right]}\geq 1-\frac{\sigma^2}{2^{2n}}\cdot\varepsilon(\tau), \tag{10}$$

where

$$\varepsilon(\tau)\stackrel{\text{def}}{=}\sum_{\mathcal{C}\in\mathsf{Comp}(\mathcal{G}_\tau)}|\mathcal{C}|^2.$$

We define $\bar{\varepsilon}$ by extending the domain of ε to Γ; $\bar{\varepsilon}(\tau)=\varepsilon(\tau)$ if τ is good, and $\bar{\varepsilon}(\tau)=0$ otherwise.

Lemma 11. *If* $\sum_{N\in\mathcal{N}_m}s_N^2\leq 2^{n-1}$*, then*

$$\mathsf{Ex}\left[\bar{\varepsilon}\right]\leq 4\sigma l+2\mu^2l^2,$$

where the expectation is taken over the distribution T_{id} *in the ideal world.*

Proof. We define a random variable S over Γ such that $S(\tau)\geq\bar{\varepsilon}(\tau)$ for any attainable transcript τ.

- For $(N,N')\in\mathcal{N}^{*2}$, we define a random variable $I_{N,N'}:\Gamma\to\{0,1\}$. For $\tau\in\Gamma$, $I_{N,N'}(\tau)=1$ if, for a positive integer t, there exists $(N[0],\ldots,N[t])\in{\mathcal{N}_m}^{*(t+1)}$ such that $N[0]=N$, $N[t]=N'$, and $\mathcal{V}_{N[i]}\cap\mathcal{V}_{N[i+1]}\neq\emptyset$ for $i=0,\ldots,t-1$; $I_{N,N'}(\tau)=0$ otherwise.
- For $N\in\mathcal{N}$, we define a random variable $\bar{s}_N$ on Γ; for $\tau\in\Gamma$, $\bar{s}_N(\tau)=s_N$ if $N\in\mathcal{N}_m$, and $\bar{s}_N(\tau)=0$ otherwise.

– Finally, let

$$S \stackrel{\text{def}}{=} \sum_{N \in \mathcal{N}} \bar{s}_N^2 + \sum_{(N,N') \in \mathcal{N}^{*2}} \bar{s}_N \bar{s}_{N'} I_{N,N'}.$$

Then for a good transcript τ, we have

$$S(\tau) = \sum_{N \in \mathcal{N}_m} s_N^2 + \sum_{(N,N') \in \mathcal{N}_m^{*2}} s_N s_{N'} I_{N,N'}.$$

Suppose that $\mathcal{N}_m = \{N_1, N_2\}$. If $\mathcal{T}_{N_1}$ and $\mathcal{T}_{N_2}$ are distinct components (i.e., $I_{N_1,N_2} = 0$), then $\sum_{\mathcal{C} \in \mathsf{Comp}(\mathcal{G}_\tau)} |\mathcal{C}|^2 = s_{N_1}^2 + s_{N_2}^2$, and otherwise,

$$\sum_{\mathcal{C} \in \mathsf{Comp}(\mathcal{G}_\tau)} |\mathcal{C}|^2 \le (s_{N_1} + s_{N_2})^2 = s_{N_1}^2 + s_{N_2}^2 + I_{N_1,N_2} s_{N_1} s_{N_2} + I_{N_2,N_1} s_{N_2} s_{N_1}.$$

By generalizing this observation, we have

$$\sum_{\mathcal{C} \in \mathsf{Comp}(\mathcal{G}_\tau)} |\mathcal{C}|^2 \le S(\tau).$$

Any attainable transcript τ is partitioned as $\tau = (\tau_1, \tau_2)$, where

$$\begin{aligned} \tau_1 &= (N_i, m_i, T_i, Z_i[1] \parallel \cdots \parallel Z_i[m_i])_{i \in [q]}, \\ \tau_2 &= (\Delta_i)_{i \in [q]}. \end{aligned}$$

A set of partial transcripts τ_1 (resp. τ_2) obtained from attainable transcripts will be denoted Γ_1 (resp. Γ_2). Let T_1 and T_2 denote the marginal distributions of τ_1 and τ_2, respectively, in the ideal world. So the joint probability distribution of T_1 and T_2 becomes T_{id}.

First, fix $\tau_1 \in \Gamma_1$. Then it determines $\mathcal{N}_m$. So we have

$$S = \sum_{N \in \mathcal{N}_m} s_N^2 + \sum_{(N,N') \in \mathcal{N}_m^{*2}} s_N s_{N'} I_{N,N'}.$$

For distinct nonces $N, N' \in \mathcal{N}_m$ and for a positive integer t, let

$$\mathcal{P}_t(N, N') \stackrel{\text{def}}{=} \left\{ (N[0], \ldots, N[t]) \in {\mathcal{N}_m}^{*(t+1)} : N[0] = N, N[t] = N' \right\}.$$

Then, we have

$$\begin{aligned} \mathsf{Ex}_{\mathsf{T}_2}[I_{N,N'}] &\le \sum_{t=1}^{|\mathcal{N}_m|-1} \sum_{(N[0],\ldots,N[t]) \in \mathcal{P}_t(N,N')} \Pr\left[\bigwedge_{i=0}^{t-1} (\mathcal{V}_{N[i]} \cap \mathcal{V}_{N[i+1]} \neq \emptyset) \right] \\ &\le \sum_{t=1}^{|\mathcal{N}_m|-1} \sum_{(N[0],\ldots,N[t]) \in \mathcal{P}_t(N,N')} \prod_{i=0}^{t-1} \frac{s_{N[i]} s_{N[i+1]}}{2^n} \\ &\le \sum_{t=1}^{\infty} \frac{s_N s_{N'}}{2^n} \left(\frac{\sum_{N'' \in \mathcal{N}_m} s_{N''}^2}{2^n} \right)^{t-1} \le \frac{2 s_N s_{N'}}{2^n}, \end{aligned}$$

where the expectation is taken over the distribution T_2. By Property 1, we have

$$\begin{aligned}
\mathsf{Ex}_{\mathsf{T}_2}[S] &= \sum_{N\in\mathcal{N}_m} s_N^2 + \sum_{(N,N')\in(\mathcal{N}_m)^{*2}} s_N s_{N'} \mathsf{Ex}_{\mathsf{T}_2}[I_{N,N'}] \\
&\le \sum_{N\in\mathcal{N}_m} s_N^2 + \sum_{(N,N')\in(\mathcal{N}_m)^{*2}} \frac{2s_N^2 s_{N'}^2}{2^n} \\
&\le \sum_{N\in\mathcal{N}_m} s_N^2 + \sum_{N\in\mathcal{N}_m} s_N^2 \left(\frac{\sum_{N'\in\mathcal{N}_m} 2s_{N'}^2}{2^n}\right) \\
&\le \sum_{N\in\mathcal{N}_m} 2s_N^2 \le 4\sigma l + 2\mu^2 l^2,
\end{aligned}$$

where the expectation is also taken over the distribution of T_2. Since the above inequality holds for any $\tau_1 \in \Gamma_1$, we also have $\mathsf{Ex}[S] \le 4\sigma l + 2\mu^2 l^2$. The proof is complete since $\mathsf{Ex}[\bar{\varepsilon}] \le \mathsf{Ex}[S]$. □

By Lemma 1, 10 and 11, and (10), we have

$$\mathsf{Adv}^{\mathsf{prg}}_{\mathsf{SCM.PRNG}^{\#}}(\mu, q, \sigma, l) \le \frac{4\sigma^3 l + 2\sigma^2\mu^2 l^2}{2^{2n}} + \frac{8\sigma l + 4\mu^2 l^2}{2^n},$$

where the right-hand side of the above inequality is greater than 1 when $2^{n-1} < \sum_{N\in\mathcal{N}_m} s_N^2$ by Property 1.

4.5 Proof of Lemma 8

Let $\mathcal{D}$ be a (μ, q, σ, l)-adversary against the pseudorandomness of $\mathsf{SCM.PRNG}^{\#}$. By giving more power to $\mathcal{D}$, we will assume that $\mathcal{D}$ makes exactly $\mu + 1$ queries for each nonce, whose length is exactly l blocks of n bits, using exactly q distinct nonces. Since $\mathcal{D}$ makes the maximum number of queries for each nonce, and since each nonce is fed to random functions ρ and ρ', generating independent masks, we can assume that $\mathcal{D}$ is *non-adapative* using a fixed set of q distinct nonces. The set of nonces will be denoted $\mathcal{N}_m = \{N_1, \ldots, N_q\}$.

At the end of the interaction, $\mathcal{D}$ will be given $\Delta_i \stackrel{\text{def}}{=} \rho(N_i)$, $i \in [q]$, for free. In the ideal world, dummy masks Δ_i will be defined by an independent random function $\rho : \mathcal{N} \to \{0,1\}^n$, and given to $\mathcal{D}$. Then the transcript is defined as

$$\tau \stackrel{\text{def}}{=} (N_i, \Delta_i, T_i, Z_i[1] \,\|\, \cdots \,\|\, Z_i[l])_{i\in[\bar{q}]},$$

where $\bar{q} = (\mu + 1)q$. For our security proof, we will partition this transcript as $\tau = (\tau', \tau'')$, where

$$\begin{aligned}
\tau' &\stackrel{\text{def}}{=} (N_i, \Delta_i, T_i)_{i\in[\bar{q}]}\,, \\
\tau'' &\stackrel{\text{def}}{=} (Z_i[1] \,\|\, \cdots \,\|\, Z_i[l])_{i\in[\bar{q}]}\,.
\end{aligned}$$

A set of partial transcripts τ' (resp. τ'') obtained from attainable transcripts will be denoted $\mathit{\Gamma}'$ (resp. $\mathit{\Gamma}''$). Let T' and T'' denote the marginal distributions of τ' and τ'', respectively, in the ideal world. We note that T' and T'' are independent.

For $i \in [\bar{q}]$ and $\alpha \in [l]$, one can fix $X_i = X_i[1] \,\|\, \cdots \,\|\, X_i[l]$, where $X_i[\alpha] = T_i \oplus 2^{\alpha-1}\Delta_i$. Let

$$\mathcal{V} = \{\pi(X_i[\alpha]) : i \in [\bar{q}], \alpha \in [l]\}\,.$$

For $N \in \mathcal{N}_m$, let

$$\mathcal{V}_N = \{\pi(X_i[\alpha]) : N_i = N, i \in [\bar{q}], \alpha \in [l]\}\,.$$

For simplicity of notation, we rename the elements of $\mathcal{V}_N$, writing

$$\mathcal{V}_N = \{V_N[1], \ldots, V_N[s]\}\,,$$

where $s = (\mu+1)l$. For $V_N[\alpha] \in \mathcal{V}_N$ such that $V_N[\alpha] = \pi(X_i[\beta])$, let $W_N[\alpha]$ denote the corresponding keysteam block $Z_i[\beta]$. This means that $W_N[\alpha] = V_N[\alpha] \oplus \rho'(N)$. We note that $\mathcal{V}_N$ and $\mathcal{V}$ are defined only by τ'. We will call a partial transcript τ' *bad* if the following condition holds.

- $\mathsf{bad} \Leftrightarrow \bigvee_{t\geq 1} \mathsf{bad}[t]$, where $\mathsf{bad}[t]$ if and only if there exist $(N[i])_{i\in[t]} \in \mathcal{N}_m^{*t}$, $(\alpha_i)_{i\in[t]}$ and $(\beta_i)_{i\in[t]}$ such that $\alpha_i \neq \beta_i$ and

  $$V_{N[i]}[\beta_i] = V_{N[i+1]}[\alpha_{i+1}]$$

  for $i = 1, \ldots, t$, with indices taken modulo t.

The subset of bad parts τ' in $\mathit{\Gamma}'$ will be denoted $\mathit{\Gamma}'_{\mathsf{bad}}$. Similarly to Lemma 10, we can prove the following lemma.

Lemma 12. $\Pr[\mathsf{T}' \in \mathit{\Gamma}'_{\mathsf{bad}}] \leq \frac{2q(\mu+1)^2l^2}{2^n}$.

We will call $\tau = (\tau', \tau'')$ a *good* transcript if τ' is not bad. Given a good transcript τ, we can define a tree $\mathcal{T}_N = (\mathcal{V}_N, \mathcal{E}_N^{=})$, and a label function λ_N on $\mathcal{E}_N^{=}$ for each nonce $N \in \mathcal{N}_m$, where any vertex $V_N[\alpha]$ such that $\alpha \geq 2$ is connected with $V_N[1]$, and

$$\lambda_N(V_N[1], V_N[\alpha]) \stackrel{\text{def}}{=} W_N[1] \oplus W_N[\alpha].$$

We also define a graph $\mathcal{G}_{\tau'} = (\mathcal{V}, \mathcal{E}^{=})$ and a label function $\lambda : \mathcal{E}^{=} \to \{0,1\}^n$ as the union of $\mathcal{T}_N$ and the union of λ_N over all nonces in $\mathcal{N}$, respectively. We note that $\mathcal{G}_{\tau'}$ is determined only by τ' (independent of τ''). We also see that there is no cycle in $\mathcal{G}_{\tau'}$ since otherwise we have bad. Similarly to the proof of Lemma 7, we have

$$\Pr[\mathsf{T}_{\mathsf{re}} = \tau] = \frac{1}{2^{(\bar{q}+2q)n}} \cdot \frac{h(\mathcal{G}_{\tau'}, \lambda)}{(2^n)_{|\mathcal{V}|}},$$
$$\Pr[\mathsf{T}_{\mathsf{id}} = \tau] = \frac{1}{2^{(q+\bar{q}+\bar{q}l)n}} = \frac{1}{2^{(|\mathcal{E}^{=}|+\bar{q}+2q)n}},$$

since $|\mathcal{E}^{=}| = \bar{q}l - q$. Therefore, we have

$$\begin{aligned}\|\mathsf{T}_{\mathsf{re}} - \mathsf{T}_{\mathsf{id}}\| &= \frac{1}{2}\sum_{\tau} |\Pr[\mathsf{T}_{\mathsf{re}} = \tau] - \Pr[\mathsf{T}_{\mathsf{id}} = \tau]| \\ &\le \frac{1}{2}\Pr[\mathsf{T}' \in \Gamma'_{\mathsf{bad}}] + \frac{1}{2}\sum_{\tau' \notin \Gamma'_{\mathsf{bad}}} \sum_{\tau'' \in \Gamma''} |\Pr[\mathsf{T}_{\mathsf{re}} = \tau] - \Pr[\mathsf{T}_{\mathsf{id}} = \tau]| \\ &= \frac{q(\mu+1)^2 l^2}{2^n} + \frac{1}{2}\sum_{\tau' \notin \Gamma'_{\mathsf{bad}}} \sum_{\tau'' \in \Gamma''} \frac{1}{2^{(\bar{q}+2q)n}} \left| \frac{h(\mathcal{G}_{\tau'}, \lambda)}{(2^n)_{|\mathcal{V}|}} - \frac{1}{2^{|\mathcal{E}^{=}|n}} \right|. \quad (11)\end{aligned}$$

For each $\lambda \in \mathcal{L}(\mathcal{G}_{\tau'})$ (which is the set of all possible label functions on $\mathcal{G}_{\tau'}$), the number of partial transcripts τ'' yielding λ is exactly 2^{qn} since one can arbitrarily choose $W_N[1]$ for each $N \in \mathcal{N}_m$. Therefore, for a fixed $\tau' \notin \Gamma'_{\mathsf{bad}}$, we have

$$\begin{aligned}\frac{1}{2}\sum_{\tau'' \in \Gamma''} \left| \frac{h(\mathcal{G}_{\tau'}, \lambda)}{(2^n)_{|\mathcal{V}|}} - \frac{1}{2^{|\mathcal{E}^{=}|n}} \right| &= \frac{1}{2}\sum_{\lambda \in \mathcal{L}(\mathcal{G}_{\tau'})} 2^{qn} \left| \frac{h(\mathcal{G}_{\tau'}, \lambda)}{(2^n)_{|\mathcal{V}|}} - \frac{1}{2^{|\mathcal{E}^{=}|n}} \right| \\ &\le 2^{qn} \cdot \varepsilon(\tau')\end{aligned}$$

where

$$\varepsilon(\tau') \stackrel{\text{def}}{=} \left(\frac{4\bar{q}l}{2^{2n}} \sum_{\mathcal{C} \in \mathsf{Comp}(\mathcal{G}_{\tau'})} |\mathcal{C}|^3 \right)^{\frac{1}{2}} + \sum_{\mathcal{C} \in \mathsf{Comp}(\mathcal{G}_{\tau'})} \frac{|\mathcal{C}|^2}{2^{n+1}} \quad (12)$$

by Lemma 4 with $\sigma \le \bar{q}l$, where $\mathsf{Comp}(\mathcal{G}_{\tau'})$ denotes the set of connected components of $\mathcal{G}_{\tau'}$. We define $\bar{\varepsilon}$ by extending the domain of ε to Γ'; $\bar{\varepsilon}(\tau') = \varepsilon(\tau')$ if $\tau' \in \Gamma' \setminus \Gamma'_{\mathsf{bad}}$, and $\bar{\varepsilon}(\tau') = 0$ otherwise. By (11) and (12), we have

$$\|\mathsf{T}_{\mathsf{re}} - \mathsf{T}_{\mathsf{id}}\| \le \frac{q(\mu+1)^2 l^2}{2^n} + \mathsf{Ex}_{\mathsf{T}'}[\bar{\varepsilon}], \quad (13)$$

where the expectation is taken over the distribution T'.

Lemma 13. *If $q(\mu+1)^2 l^2 \le 2^{n-1}$, then*

$$\mathsf{Ex}_{\mathsf{T}'}[\bar{\varepsilon}] \le \frac{7q(\mu+1)^2 l^2}{2^n}.$$

Proof. We define some random variables to upper bound $\bar{\varepsilon}$ as follows.

– For $(N, N') \in {\mathcal{N}_m}^{*2}$, we define a random variable $I_{N,N'} : \Gamma' \to \{0,1\}$. For $\tau' \in \Gamma'$, $I_{N,N'}(\tau') = 1$ if, for a positive integer t, there exists

$$(N[0], \ldots, N[t]) \in {\mathcal{N}_m}^{*(t+1)}$$

such that $N[0] = N$, $N[t] = N'$, and $\mathcal{V}_{N[i-1]} \cap \mathcal{V}_{N[i]} \neq \emptyset$ for $i \in [t]$; $I_{N,N'}(\tau') = 0$ otherwise. If $\tau = (\tau', \tau'')$ is good, and $I_{N,N'}(\tau') = 1$, then two trees $\mathcal{T}_N$ and $\mathcal{T}_{N'}$ are in the same component of $\mathcal{G}_{\tau'}$.

– For $(N, N', N'') \in {\mathcal{N}_m}^{*3}$, we define a random variable $J_{N,N',N''} : \Gamma' \to \{0,1\}$. For $\tau' \in \Gamma'$, $J_{N,N',N''}(\tau') = 1$ if, for integers $t \geq 1$ and $t' \geq 0$, there exist two sequences of nonces

$$(N[0], \ldots, N[t]) \in {\mathcal{N}_m}^{*(t+1)},$$

$$(N'[0], \ldots, N'[t']) \in {\mathcal{N}_m}^{*(t'+1)}$$

such that $N[0] = N$, $N[t] = N''$, $N'[t'] = N'$, $\mathcal{V}_{N[i-1]} \cap \mathcal{V}_{N[i]} \neq \emptyset$ for $i \in [t]$, $\mathcal{V}_{N'[i-1]} \cap \mathcal{V}_{N'[i]} \neq \emptyset$ for $i \in [t']$, and

$$\{N[0], \ldots, N[t]\} \cap \{N'[0], \ldots, N'[t']\} = \{N'[0]\};$$

$J_{N,N',N''}(\tau') = 0$ otherwise. If $\tau = (\tau', \tau'')$ is good, and $J_{N,N',N''}(\tau') = 1$, then three trees $\mathcal{T}_N$, $\mathcal{T}_{N'}$ and $\mathcal{T}_{N''}$ are in the same component of $\mathcal{G}_{\tau'}$.

– Let

$$S(\tau') \stackrel{\text{def}}{=} qs^2 + \sum_{(N,N') \in {\mathcal{N}_m}^{*2}} s^2 I_{N,N'}(\tau'),$$

$$T(\tau') \stackrel{\text{def}}{=} qs^3 + 3 \sum_{(N,N') \in {\mathcal{N}_m}^{*2}} s^3 I_{N,N'}(\tau') + \sum_{(N,N',N'') \in {\mathcal{N}_m}^{*3}} s^3 J_{N,N',N''}(\tau').$$

Then for any $\tau' \in \Gamma' \setminus \Gamma'_{\mathsf{bad}}$, we have

$$\sum_{\mathcal{C} \in \mathsf{Comp}(\mathcal{G}_{\tau'})} |\mathcal{C}|^2 \leq S(\tau'), \qquad \sum_{\mathcal{C} \in \mathsf{Comp}(\mathcal{G}_{\tau'})} |\mathcal{C}|^3 \leq T(\tau'). \tag{14}$$

For any $\tau' \in \Gamma'$, let $\tau' = (\tau_1, \tau_2)$, where $\tau_1 = (N_i, T_i)_{i \in [\bar{q}]}$ and $\tau_2 = (\Delta_i)_{i \in [\bar{q}]}$. A set of partial transcripts τ_1 (resp. τ_2) obtained from the transcripts in Γ' will be denoted Γ_1 (resp. Γ_2). Let T_1 and T_2 denote the marginal distributions of τ_1 and τ_2, respectively, in the ideal world.

Similarly to the proof of Lemma 11, we have $\mathsf{Ex}_{\mathsf{T}_2}[I_{N,N'}] = \frac{2s^2}{2^n}$ for any $\tau_1 \in \Gamma_1$, and hence,

$$\mathsf{Ex}_{\mathsf{T}'}[S] \leq 2q(\mu+1)^2 l^2. \tag{15}$$

The next goal is to upper bound $\mathsf{Ex}_{\mathsf{T}'}[T]$; we fix $\tau_1 \in \Gamma_1$. For distinct nonces $N, N', N'' \in \mathcal{N}_m$, integers $t \geq 1$ and $t' \geq 0$, the number of sequences $(N[i]) \in {\mathcal{N}_m}^{*(t+1)}$ and $(N'[i]) \in {\mathcal{N}_m}^{*(t'+1)}$ such that $N[0] = N$, $N[t] = N''$, $N'[0] = N[j]$ for some $j \in \{0, \ldots, t\}$, and $N'[t'] = N'$ is at most $(t+1)q^{t+t'-2}$, where it cannot be the case that both $t = 1$ and $t' = 0$. For each of such sequences, we have $\mathcal{V}_{N[i-1]} \cap \mathcal{V}_{N[i]} \neq \emptyset$ for $i \in [t]$, and $\mathcal{V}_{N'[i-1]} \cap \mathcal{V}_{N'[i]} \neq \emptyset$ for $i \in [t']$ with probability at most $\left(\frac{s^2}{2^n}\right)^{t+t'}$. Therefore, we have

$$\begin{aligned}
\mathsf{Ex}_{\mathsf{T}_2}[J_{N,N',N''}] &\leq \sum_{t'=1}^{\infty} \left(2q^{t'-1}\left(\frac{s^2}{2^n}\right)^{t'+1}\right) + \sum_{t=2}^{\infty}\sum_{t'=0}^{\infty}\left((t+1)q^{t+t'-2}\left(\frac{s^2}{2^n}\right)^{t+t'}\right) \\
&\leq \frac{4s^4}{2^{2n}} + \frac{s^4}{2^{2n}} \sum_{t=0}^{\infty}\left((t+3)\left(\frac{qs^2}{2^n}\right)^t \sum_{t'=0}^{\infty}\left(\frac{qs^2}{2^n}\right)^{t'}\right) \leq \frac{20s^4}{2^{2n}},
\end{aligned}$$

where the expectation is taken over the distribution T_2 and the last inequality holds since $qs^2 \le 2^{n-1}$. By (14) and since $\mathsf{Ex}_{\mathsf{T}_2}[I_{N,N'}] \le \frac{2s^2}{2^n}$, we have

$$\mathsf{Ex}_{\mathsf{T}_2}[T] \le qs^3 + \frac{6q^2s^5}{2^n} + \frac{20q^3s^7}{2^{2n}} \le 9qs^3 = 9q(\mu+1)^3l^3$$

where the expectation is also taken over the distribution T_2. Since the above inequality holds for any $\tau_1 \in \Gamma_1$, we have

$$\mathsf{Ex}_{\mathsf{T}'}[T] \le 9q(\mu+1)^3l^3. \tag{16}$$

By (12), (14), (15), (16) and Jensen's inequality, we have

$$\begin{aligned}\mathsf{Ex}_{\mathsf{T}'}[\bar{\varepsilon}] &\le \left(\frac{4\bar{q}l\mathsf{Ex}_{\mathsf{T}'}[T]}{2^{2n}}\right)^{\frac{1}{2}} + \frac{\mathsf{Ex}_{\mathsf{T}'}[S]}{2^{n+1}} \\ &\le \left(\frac{36q^2(\mu+1)^4l^4}{2^{2n}}\right)^{\frac{1}{2}} + \frac{q(\mu+1)^2l^2}{2^n} \le \frac{7q(\mu+1)^2l^2}{2^n}.\end{aligned}$$

□

By (13) and Lemma 13, we have

$$\mathsf{Adv}^{\mathsf{prg}}_{\mathsf{SCM.PRNG}^*}(q,\mu,\sigma,l) \le \|\mathsf{T}_{\mathsf{re}} - \mathsf{T}_{\mathsf{id}}\| \le \frac{8q(\mu+1)^2l^2}{2^n}.$$

4.6 Using Random IVs

One may want to instantiate nonces with random IVs for convenience of implementation. For the analysis of this instantiation, we need to introduce a new parameter r that denotes the highest multiplicity in IV collisions. Then we make the following observations.

1. The expected number of IV collisions is $\frac{q(q-1)}{2^{n-1}}$. By defining $\mu > q^{\frac{2}{3}}$ as a bad event, one can upper bound μ by $q^{\frac{2}{3}}$, while the probability of this bad event is upper bounded by $\frac{2q^{\frac{4}{3}}}{2^n}$ by Markov's inequality. Following the proof of Lemma 6 with this bad event, we have

$$\mathsf{Adv}^{\mathsf{mac}}_{\mathsf{SCM.MAC}^*[H]}(q,v) \le \frac{16q^{\frac{8}{3}}}{2^{2n}} + \frac{3q^{\frac{4}{3}}}{2^n} + 4q^{\frac{4}{3}}\delta + \frac{4v}{2^n} + (2L+1)v\delta + 2^n\left(\frac{eq^{\frac{4}{3}}}{L2^n}\right)^L.$$

2. By closely looking at the proof of Lemma 7, one see that

$$\mathsf{Adv}^{\mathsf{prg}}_{\mathsf{SCM.PRNG}^{\#}}(\mu,q,\sigma,l) \le \frac{2\sigma^2S}{2^{2n}} + \frac{4S}{2^n}$$

where $S = \max_{\tau\in\Gamma}\left\{\sum_{N\in\mathcal{N}_m} s_N^2\right\}$. Since $\sum_{N\in\mathcal{N}_m} s_N^2 \le \sigma rl$ and $\Pr[r \ge 4] \le 3q^4/2^{3n}$, we have

$$\mathsf{Adv}^{\mathsf{prg}}_{\mathsf{SCM.PRNG}^{\#}}(q,\sigma,l) \le \frac{6\sigma^3l}{2^{2n}} + \frac{12\sigma l}{2^n} + \frac{3q^4}{2^{3n}}.$$

3. In the proof of Lemma 8, it is assumed that exactly $\mu + 1$ queries are made for each nonce. When nonces are instantiated with random IVs, $\mu + 1$ can be replaced by r, obtaining the following bound.

$$\mathsf{Adv}^{\mathsf{prg}}_{\mathsf{SCM.PRNG}^{\#}}(q, \sigma, l) \leq \frac{72ql^2}{2^n} + \frac{3q^4}{2^{3n}}.$$

All in all, we conclude that the security bound is dominated by

$$\min\left\{\frac{72ql^2}{2^n}, \frac{6\sigma^3 l}{2^{2n}} + \frac{12\sigma l}{2^n}\right\},$$

when $q \ll O(2^{\frac{3n}{4}})$ and $v \ll O(2^n)$.

References

[1] Elena Andreeva, Andrey Bogdanov, Nilanjan Datta, Atul Luykx, Bart Mennick, Mridul Nandi, Elmar Tischhauser, and Kan Yasuda. COLM v1. Submission to the CAESAR competition, 2016. Available at https://competitions.cr.yp.to/round3/colmv1.pdf.

[2] Mihir Bellare, Phillip Rogaway, and David Wagner. The EAX Mode of Operation. In Bimal Roy and Willi Meier, editors, *Fast Software Encryption - FSE 2004*, volume 3017 of *LNCS*, pages 389–407. Springer, 2004.

[3] Srimanta Bhattacharya and Mridul Nandi. Revisiting Variable Output Length XOR Pseudorandom Function. *IACR Transactions on Symmetric Cryptology*, 2018, Issue 1:314–335, 2018.

[4] Priyanka Bose, Viet Tung Hoang, and Stefano Tessaro. Revisiting AES-GCM-SIV: Multi-user security, faster key derivation, and better bounds. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018*, LNCS, pages 468–499. Springer, 2018.

[5] Wonseok Choi, Byeonghak Lee, Yeongmin Lee, and Jooyoung Lee. Improved Security Analysis for Nonce-based Enhanced Hash-then-Mask MACs. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020*, volume 12491 of *LNCS*, pages 697–723. Springer, 2020.

[6] Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Kan Yasuda. Encrypt or Decrypt? To Make a Single-Key Beyond Birthday Secure Nonce-Based MAC. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 (Proceedings, Part I)*, volume 10991 of *LNCS*, pages 631–661. Springer, 2018.

[7] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2. Submission to the CAESAR competition, 2016. Available at https://competitions.cr.yp.to/round3/asconv12.pdf.

[8] Avijit Dutta, Mridul Nandi, and Suprita Talnikar. Beyond Birthday Bound Secure MAC in Faulty Nonce Model. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 (Proceedings, Part I)*, volume 11476 of *LNCS*, pages 437–466. Springer, 2019.

[9] Shay Gueron, Adam Langley, and Yehuda Lindell. AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption. RFC 8452, April 2019.

[10] Shay Gueron and Yehuda Lindell. GCM-SIV: Full Nonce Misuse-Resistant Authenticated Encryption at Under One Cycle per Byte. In Indrajit Ray, editor, *ACM SIGSAC Conference on Computer and Communications Security - CCS 2015*, pages 109–119. Association for Computing Machinery, 2015.

[11] Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway. Robust Authenticated-Encryption AEZ and the Problem That It Solves. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 (Proceedings, Part I)*, volume 9056 of *LNCS*, pages 15–44. Springer, 2015.

[12] Viet Tung Hoang and Stefano Tessaro. Key-Alternating Ciphers and Key-Length Extension: Exact Bounds and Multi-user Security. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 (Proceedings, Part I)*, volume 9814 of *LNCS*, pages 3–32. Springer, 2016.

[13] Tetsu Iwata. Authenticated Encryption Mode for Beyond the Birthday Bound Security. In Serge Vaudenay, editor, *Progress in Cryptology - AFRICACRYPT 2008*, volume 5023 of *LNCS*, pages 125–142. Springer, 2008.

[14] Tetsu Iwata and Kazuhiko Minematsu. Stronger Security Variants of GCM-SIV. *IACR Transactions on Symmetric Cryptology*, 2016, Issue 1:134–157, 2016.

[15] Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin. ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 (Proceedings, Part III)*, volume 10403 of *LNCS*, pages 34–65. Springer, 2017.

[16] Tetsu Iwata and Yannick Seurin. Reconsidering the security bound of AES-GCM-SIV. *IACR Transactions on Symmetric Cryptology*, 2017, Issue 4:240–267, 2017.

[17] Jérémy Jean, Ivica Nikolić, Thomas Peyrin, and Yannick Seurin. Deoxys v1.41. Submission to the CAESAR competition, 2016. Available at https://competitions.cr.yp.to/round3/deoxysv141.pdf.

[18] Ted Krovetz and Phillip Rogaway. The Software Performance of Authenticated-Encryption Modes. In Antoine Joux, editor, *Fast Software Encryption - FSE 2011*, volume 6733 of *LNCS*, pages 306–327. Springer, 2011.

[19] Ted Krovetz and Phillip Rogaway. OCB (v1.1). Submission to the CAESAR competition, 2016. Available at https://competitions.cr.yp.to/round3/ocbv11.pdf.

[20] David A. McGrew and John Viega. The Security and Performance of the Galois/Counter Mode (GCM) of Operation. In Anne Canteaut and Kapaleeswaran Viswanathan, editors, *Progress in Cryptology - INDOCRYPT 2004*, volume 3348 of *LNCS*, pages 343–355. Springer, 2004.

[21] Yoav Nir and Adam Langley. ChaCha20 and Poly1305 for IETF protocols. RFC 7539, 2015.

[22] Jacques Patarin. Introduction to Mirror Theory: Analysis of Systems of Linear Equalities and Linear Non Equalities for Cryptography. IACR Cryptology ePrint Archive, Report 2010/287, 2010. Available at http://eprint.iacr.org/2010/287.

[23] Jacques Patarin. Mirror Theory and Cryptography. IACR Cryptology ePrint Archive, Report 2016/702, 2016. Available at http://eprint.iacr.org/2016/702.

[24] Thomas Peyrin and Yannick Seurin. Counter-in-Tweak: Authenticated Encryption Modes for Tweakable Block Ciphers. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 (Proceedings, Part I)*, volume 9814 of *LNCS*, pages 33–63. Springer, 2016.

[25] Phillip Rogaway and Thomas Shrimpton. A Provable-Security Treatment of the Key-Wrap Problem. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 373–390. Springer, 2006.

[26] Doug Whiting, Russ Housley, and Niels Ferguson. Counter with CBC-MAC (CCM). Submission to NIST, 2002. Available at https://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ccm/ccm.pdf.

[27] Hongjun Wu. ACORN: A Lightweight Authenticated Cipher (v3). Submission to the CAESAR competition, 2016. Available at https://competitions.cr.yp.to/round3/acornv3.pdf.

[28] Hongjun Wu and Bart Preneel. AEGIS: A Fast Authenticated Encryption Algorithm (v1.1). Submission to the CAESAR competition, 2016. Available at https://competitions.cr.yp.to/round3/aegisv11.pdf.