

Beyond-Birthday MAC Security for Encrypted Wegman-Carter and EWCDMD

Yuxiang Wang¹²³, Chun Guo^{123(✉)}, and Sihuang Hu^{123(✉)}

¹ School of Cyber Science and Technology, Shandong University, Qingdao, China

² State Key Laboratory of Cryptography and Digital Economy Security, Shandong University, Qingdao, 266237, China

³ Key Laboratory of Cryptologic Technology and Information Security of Ministry of Education, Shandong University, Qingdao, Shandong, 266237, China
quince773@gmail.com, chun.guo.sc@gmail.com, husihuang@gmail.com

Abstract. At CRYPTO 2016, Cogliati and Seurin proposed EWCDM as a nonce-based MAC construction making two block cipher calls and one almost-XOR-universal (AXU) hash evaluation and achieving beyond-birthday-bound (BBB) security. They noticed that a simplified variant of EWCDM named Encrypted Wegman-Carter (EWC) admits a birthday distinguishing attack. Later, at CRYPTO 2017, Mennink and Neves proposed EWCDMD, the dual of EWCDM, as a new candidate BBB-secure MAC, but at EUROCRYPT 2020 Nandi proposed a birthday distinguishing attack against EWCDMD. However, the distinguishing attacks did not yield forgeries, and whether EWC and EWCDMD have BBB unforgeability (or MAC security) remains open.

We prove beyond-birthday unforgeability for EWC and EWCDMD and answer this long-standing open problem positively. Using an n -bit block cipher and an $O(2^{-n})$ -AXU hash family, we prove that both constructions are secure up to $2^{5n/6}$ MAC queries and nearly 2^n verification queries, in the nonce-respecting setting.

To bypass the birthday distinguishing attacks, our proofs directly analyze forgery events using auxiliary experiments indexed by hash values and messages. For EWC, we additionally employ conditional permutation analysis and collision multiplicity bounds with KL divergence, whereas for EWCDMD we use Hellinger distance and Fourier analysis.

Table of Contents

Beyond-Birthday MAC Security for Encrypted Wegman-Carter and EWCDMD	1
<i>Yuxiang Wang, Chun Guo^(✉), and Sihuang Hu^(✉)</i>	
1 Introduction	2
2 Preliminaries and Security Model	7
2.1 Notation and the MAC constructions	7
2.2 Nonce-respecting MAC security	8
2.3 Tools: Distance, permutation, and reusable estimates	9
3 List Forgery	12
4 Security of EWC	16
4.1 New-nonce and non-copy repeated-nonce forgeries	17
4.2 The copy event and auxiliary experiments	20
4.3 Conditional divergence between the Real and Clr experiments...	22
4.4 The stopped KL argument	29
4.5 Completing the proof of Theorem 1	31
5 Security of EWCDMD	32
5.1 Non-copy forgeries	32
5.2 The copy event and auxiliary experiments	38
5.3 Conditional divergence between the join distributions	39
5.4 Conditional distance between the new-root tag distributions	45
5.5 The stopped Hellinger argument	49
5.6 Completing the proof of Theorem 2	53
6 Birthday Forgery Attack and MAC Security of $F_{B_2}^{\text{EDMD}}$	53
6.1 Birthday Forgery Attack Against $F_{B_2}^{\text{EDMD}}$	53
6.2 Birthday MAC Security of $F_{B_2}^{\text{EDMD}}$	59
7 Use of Generative AI Tools	62

1 Introduction

Message authentication codes (MACs) allow parties sharing a secret key to protect the authenticity and integrity of their messages. The universal-hashing approach of Wegman and Carter [27] compresses a potentially long message with a keyed hash and masks the result with a one-time pad. Brassard [2] placed this approach in a computational setting by generating the masks pseudorandomly from a short shared key. Concretely, for a nonce N and a message M , the resulting tag takes the form $F_K(N) \oplus h(M)$, where F_K is a pseudorandom function (PRF) and h is an independently keyed almost-XOR-universal (AXU) hash function [26]. This separates the cost of processing the message from that of generating the cryptographic mask. The analyses of Shoup [26] and Cogliati and Seurin [8] give strong authentication guarantees when the nonces are distinct and the masking function is a secure PRF.

Two considerations complicate this picture. First, reusing a nonce cancels the mask in the difference of two tags, exposing a difference of hash values; for common polynomial hash families, such information can lead to hash-key recovery, as illustrated by Joux’s attack on GCM [20] and the broader key-recovery analyses of Handschuh and Preneel [18]. Second, block ciphers implement pseudorandom permutations rather than arbitrary pseudorandom functions. Replacing a permutation with a random function by the PRP/PRF switching lemma [1] introduces a loss of order $q^2/2^n$, where n is the block length and q is the number of queries. The resulting birthday bound is particularly restrictive for small block sizes [8,3]. These considerations motivate efficient MACs that offer security beyond the birthday bound under normal nonce use and retain useful protection when nonce generation fails.

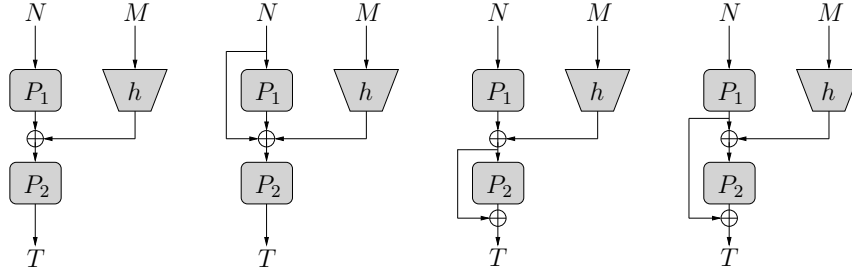


Fig. 1. Encrypted Wegman–Carter and its variants. From left to right: Encrypted Wegman–Carter (EWC) [8]; EWCDM [8]; EWCDMD [21]; $F_{B_2}^{\text{EDMD}}$ [3].

Encrypted Wegman–Carter and variants. Cogliati and Seurin (CS) [8] showed that applying an independently keyed block cipher to the Wegman–Carter tag makes it nonce-misuse resistant (up to $2^{n/2}$ authentication queries), and called the resulting construction *Encrypted Wegman–Carter (EWC)*. A standard reduction would replace the two block ciphers with two independent secret random permutations P_1, P_2 on n bits, with which the EWC construction, depicted in Fig. 1 (first from the left), is defined by

$$\text{EWC}(N, M) := P_2(P_1(N) \oplus h(M)).$$

However, this construction admits a *distinguishing attack* with $2^{n/2}$ complexity [8,16]: fixing M arbitrarily and making $\lambda \approx 2^{n/2}$ authentication queries

$$T_1 \leftarrow \text{EWC}(N_1, M), \dots, T_\lambda \leftarrow \text{EWC}(N_\lambda, M)$$

necessarily yields distinct $T_1, \dots, T_\lambda$ and enables distinguishing the EWC MAC oracle from a random function. While this does not yield a forgery, it means EWC

cannot be proven beyond-birthday secure using the CS framework [8, Sect. 4.1]. Due to this, CS added a nonce feed-forward to EWC and proposed the *Encrypted Wegman–Carter with Davies–Meyer (EWCDM)* construction, as depicted in Fig. 1 (second from the left):

$$\text{EWCDM}(N, M) := P_2(P_1(N) \oplus N \oplus h(M)).$$

Their analysis established security up to $2^{2n/3}$ authentication queries in the nonce-respecting setting, together with birthday-bound nonce-misuse resistance. Both constructions require one hash evaluation and two block cipher calls, and the first cipher call can be computed in parallel with the hash. Thanks to this nonce feed-forward, no additional block cipher calls are needed for beyond-birthday security.

CS left open the question of whether EWCDM or alternative constructions can provably achieve “full” n -bit security. To solve this, Dai et al. [11] introduced the chi-squared method and proved $3n/4$ -bit PRF security for the underlying Encrypted Davies–Meyer (EDM) construction $\text{EDM}(X) := P_2(P_1(X) \oplus X)$. However, the chi-squared method falls short of proving BBB MAC security [13], and a more promising approach is to use Patarin’s H-coefficient method [24] plus Mirror Theory [25], as pioneered by Mennink and Neves [21]. The latter approach was subsequently extended and refined in [12, 7], and Choi et al. [6] were eventually able to prove full n -bit nonce-respecting MAC security for EWCDM to completely solve CS’s open problem.

To obtain a plausible alternative construction, Mennink and Neves [21] modified the position of the feed-forward action in EWCDM to yield EWCDMD, the dual of EWCDM, as shown in Fig. 1 (third from the left):

$$\text{EWCDMD}(N, M) := P_2(P_1(N) \oplus h(M)) \oplus P_1(N) \oplus h(M).$$

Mennink and Neves attempted to use Mirror Theory to prove n -bit PRF security for EWCDMD in the nonce-respecting setting. However, Nandi [22] disproved their result by exhibiting a *distinguishing attack* against EWCDMD. His attack exploits excess collisions arising from the composition of non-injective functions, and does not lead to a forgery.

By slightly changing the “starting point” of the feed-forward in EWCDMD in Fig. 1 (third from the left), another variant shown in Fig. 1 (fourth from the left) can be obtained. In Chen et al.’s systematic categorization of two block cipher-based MACs [3], this variant was called $F_{B_2}^{\text{EDMD}}$:

$$F_{B_2}^{\text{EDMD}}(N, M) := P_2(P_1(N) \oplus h(M)) \oplus P_1(N).$$

Chen et al. discussed the security of the various two block cipher-based MACs and Choi et al. [6] further tightened the security bounds. Yet, in [3, Table 1], $F_{B_2}^{\text{EDMD}}$ was the only remaining candidate whose BBB MAC security was unknown.

Pseudorandomness vs. MAC Security. As mentioned, EWC and EWCDMD admit distinguishing attacks with birthday complexity (in the nonce-respecting

setting), i.e., with $2^{n/2}$ authentication queries, their authentication oracles can be distinguished from random functions. But the attacks do not result in forgeries. In fact, the questions of whether EWC and EWCDMD have BBB *MAC security* or *unforgeability* have been open for years: see [22]. Note that the state-of-the-art security proof paradigm is due to CS [8], which proves BBB MAC security by first proving BBB PRF security. Due to the attacks, if BBB MAC security can be proven for EWC and EWCDMD then the proof must use *a conceptually new proof paradigm*.

Our results. We give direct unforgeability analyses of EWC and EWCDMD and show that both achieve (far beyond-birthday) $5n/6$ -bit MAC security (in the nonce-respecting setting), answering the ten-year open problem. Concretely, in the nonce-respecting setting, if an $O(2^{-n})$ -almost-XOR-universal (AXU) hash function family is used, then: (i) EWC is unforgeable up to roughly $2^{5n/6}$ adaptive authentication queries and 2^n verification queries; (ii) EWCDMD is unforgeable up to roughly $2^{5n/6}$ adaptive authentication queries and $2^n/n$ verification queries.

Technical approach. We first reduce the standard MAC security experiment, in which authentication and verification queries may be adaptively interleaved, to a *list forgery* experiment (Section 3). In the latter experiment, the adversary makes all authentication queries first and then outputs a list of verification candidates, without receiving verification feedback; it succeeds if any candidate is valid. Each candidate must be fresh relative to the entire authentication transcript, whereas in the standard experiment freshness is required only relative to authentication records preceding that verification query.

The reduction simulates the standard MAC experiment by forwarding authentication queries to its authentication oracle in the list forgery experiment, answering every verification query with rejection, and recording the corresponding candidate for inclusion in the final list. Under the same secret key, the simulated and standard interactions coincide until, but not including, the first accepting verification response in the standard experiment. However, a recorded candidate may coincide with a later authentication record and thus fail the freshness requirement of the list experiment. We bound this matching event separately, at a cost of at most $v/(2^n - q + 1)$ for EWC and $(n + 1)v/(2^n - q + 1)$ for EWCDMD.

In the list experiment, using the residual uniformity of the permutations (i.e., uniform sampling from unused outputs after conditioning on the assigned permutation input-output pairs) and the conditional distribution of their internal values, we can prove that most types of forgeries are unlikely to be accepted. The main difficulty is what we call a *copy forgery*: at an old nonce, the adversary submits the observed tag for a different message with the same hash value. AXU bounds collisions between fixed messages, but the messages in this event are chosen adaptively from a transcript that depends on the secret hash key. We therefore cannot apply AXU directly after conditioning on the real transcript.

To handle copy forgeries, let *Real* denote the real authentication experiment. We introduce two auxiliary authentication experiments: *Clr* uses independent

random permutations indexed by hash values, which we call *colors*, whereas **Msg** uses independent random permutations indexed by messages. For EWC, these permutations map nonces to tags; for EWCDMD, they map nonces to internal roots, which are then transformed into tags by the common map $y \mapsto P_2(y) \oplus y$.

In the message-indexed experiment, authentication responses are generated using the permutation assigned to each message, without evaluating the hash function. Hence the resulting transcript and the adversary’s forgery candidates are independent of the hash key. Conditioned on this transcript and the candidate list, each copy forgery requires a hash collision between two fixed, distinct messages, which occurs with probability at most ε by the AXU property. A union bound over the at most v candidates therefore gives a copy probability of at most $v\varepsilon$.

The copy event depends on both the hash function and the authentication transcript. We therefore compare the joint distributions of the hash function and the authentication transcript across the three experiments. The resulting statistical distances bound the increase in the copy probability when passing from **Msg** to **Clr** and then to **Real**.

The **Msg**–**Clr** comparison yields a statistical distance of at most $\binom{q}{2}\varepsilon/2^n$. For EWC, a transcript possible in **Msg** is incompatible with **Clr** if two distinct messages have both the same hash value and the same tag: in **Clr**, equal hash values select the same permutation, which must return distinct outputs at distinct nonces. In **Msg**, the expected number of tag-colliding pairs of distinct messages is at most $\binom{q}{2}/2^n$, and each pair has equal hash values with probability at most ε . For EWCDMD, the same argument applies to the internal roots rather than the final tags.

The remaining comparison requires a precise description of the roots $Y_i := P_1(N_i) \oplus h(M_i)$, $i \in \{1, \dots, q\}$. For EWC, equal tags identify equal roots. Conditioned on the hash key and transcript, the distinct roots are uniform over tuples satisfying the input–output constraints of both permutations. A local switching argument on these tuples controls the probability that the next query joins each existing root class. On the new-root branch, both experiments return a uniform unused tag. We thus bound the chi-squared divergence through the joining probabilities and accumulate these bounds using the KL chain rule [9]. Moment bounds on collision multiplicities allow this comparison to continue well beyond the first collision.

For EWCDMD, distinct roots can yield the same tag, so the proof retains the latent partition induced by root equality without revealing it to the adversary. The joining analysis extends to this partition, but the tag at a new root is no longer uniform over unused tags. We express its deviation from uniform as an XOR convolution involving the excluded roots and assigned P_2 outputs, and bound it by Fourier analysis. Sampling-without-replacement estimates [19] control the relevant Fourier coefficients despite adaptive queries. Since the real and auxiliary experiments induce different conditional root distributions, we compare their new-root tag laws through a common uniform distribution and combine the old-root and new-root contributions using Hellinger distance [17].

Both comparisons stop when a tag occurs more than five times. The resulting tail bounds contribute $O(q^6/2^{5n})$, while converting the accumulated divergence to statistical distance contributes $O(q^3/2^{5n/2})$ among the terms in the final bounds. Combining these list-forgery bounds with the aforementioned standard-to-list reduction gap, when $\varepsilon = O(2^{-n})$ we obtain the claims: EWC security up to $2^{5n/6}$ authentication queries and 2^n verification queries, and EWCDMD security up to $2^{5n/6}$ authentication queries and $2^n/n$ verification queries.

Finally, to complete the BBB picture of Chen et al.'s characterization [3], we also show a birthday forgery attack against $F_{B_2}^{\text{EDMD}}$. Concretely, over $\mathbb{F}_{2^n}$ we exhibit the 2^{1-n} -AXU family $h_\alpha(x, y) := \alpha x \oplus \alpha^2 y$. For this family and $n \geq 64$, Theorem 3 gives a nonce-respecting forgery attack using $q = \Theta(2^{n/2} \sqrt{n})$ authentication queries and a single verification candidate, with success probability greater than $1/42$. This means $F_{B_2}^{\text{EDMD}}$ cannot achieve BBB security under the AXU assumption alone. We do not view this as our main result. As a complementary result, we prove birthday MAC security for $F_{B_2}^{\text{EDMD}}$.

Related work. Datta et al. [13] proposed Decrypted Wegman–Carter with Davies–Meyer (DWCDM), replacing the outer encryption in EWCDM with decryption so that both cipher calls can use the same key: $\text{DWCDM}(N, M) := E_K^{-1}(E_K(N) \oplus N \oplus h(M))$. They proved $2n/3$ -bit nonce-respecting MAC security and birthday-bound nonce-misuse resistance, which was improved to $3n/4$ -bit security in [12]. Dutta et al. [16] formalized the faulty nonce model, which measures security as a function of the number of authentication queries that reuse a nonce, and proposed the nonce-based Enhanced Hash-then-Mask (nEHtM) MAC with $2n/3$ -bit nonce-respecting MAC security, and Choi et al. [5] further improved the analysis of nEHtM to $3n/4$ -bit MAC security. As a limitation, EWC and EWCDMD do not have BBB security in the faulty nonce model.

Organization. Section 2 introduces the security model and probabilistic tools. Section 3 introduces the list forgery experiment and reduces MAC advantage to list forgery advantage up to an additive bad-event term. Sections 4 and 5 establish the EWC and EWCDMD bounds, respectively. Section 6 presents a birthday-bound forgery attack against $F_{B_2}^{\text{EDMD}}$ and establishes a MAC security bound.

2 Preliminaries and Security Model

2.1 Notation and the MAC constructions

Let $n \geq 1$, and identify $\mathbb{F}_2^n$ with $\{0, 1\}^n$, so $|\mathbb{F}_2^n| = 2^n$. Write $(2^n)_k := 2^n(2^n - 1) \cdots (2^n - k + 1)$, with $(2^n)_0 := 1$. Also, $[k] := \{1, \dots, k\}$ and $[0] := \emptyset$. Addition in $\mathbb{F}_2^n$ is bitwise XOR. The permutations $P_1, P_2 \leftarrow_{\$} \text{Perm}(\mathbb{F}_2^n)$ are independent and uniform. Let $\mathcal{M}$ be a nonempty message space, and let $\mathcal{H}$ be a finite ε -almost-XOR-universal family of functions from $\mathcal{M}$ to $\mathbb{F}_2^n$. Independently of P_1, P_2 , sample

$h \xleftarrow{\$} \mathcal{H}$. Thus, for all distinct M, M' and every $\delta \in \mathbb{F}_2^n$,

$$\Pr_h[h(M) \oplus h(M') = \delta] \leq \varepsilon. \quad (1)$$

For a random variable X , $\mathcal{L}(X)$ denotes its distribution. A subscript identifies the governing experiment or probability law. For example, $\mathcal{L}_W(X)$ denotes the distribution of X in experiment W . When a random variable and its value use the same symbol and appear together, we use boldface for the random variable, as in $\mathbf{h} = h$. For a fixed value X , we write $\Pr[\cdot \mid X]$ for $\Pr[\cdot \mid \mathbf{X} = X]$ when unambiguous. The same convention applies to tuples, conditional distributions, and conditional expectations.

For a nonce $N \in \mathbb{F}_2^n$ and a message $M \in \mathcal{M}$, the three nonce-based MACs analyzed in this work are

$$\text{EWC}(N, M) := P_2(P_1(N) \oplus h(M)), \quad (2)$$

$$\text{EWCDMD}(N, M) := P_2(P_1(N) \oplus h(M)) \oplus P_1(N) \oplus h(M), \quad (3)$$

$$F_{B_2}^{\text{EDMD}}(N, M) := P_2(P_1(N) \oplus h(M)) \oplus P_1(N). \quad (4)$$

2.2 Nonce-respecting MAC security

Let MAC_K be a deterministic nonce-based MAC with n -bit nonces and tags. The challenger samples a secret key K once from a finite key space and provides an adversary $\mathcal{A}$ with two oracles. An authentication query (N, M) to Tag_K returns $\text{MAC}_K(N, M)$. A verification query (N, M, T) to Vrfy_K returns $b = 1$ if $T = \text{MAC}_K(N, M)$, and otherwise returns $b = 0$. For the constructions in Equations (2) to (4), $K := (P_1, P_2, h)$. The adversary has access only to these two oracles, and the permutations and the hash key remain secret.

We consider information-theoretic security. Adversaries are computationally unbounded. A (q, v) -adversary makes at most q authentication queries and at most v verification queries. At each step, the adversary determines the query type and its contents based on all preceding queries and responses. Write (N_i, M_i, T_i) for the i -th authentication record, and (N'_j, M'_j, T'_j, b_j) for the j -th verification record. Authentication nonces are distinct. Let t_j denote the number of authentication queries preceding the j -th verification query. Each verification query j must satisfy

$$(N'_j, M'_j, T'_j) \neq (N_i, M_i, T_i) \quad \text{for every } i \in [t_j]. \quad (5)$$

The adversary succeeds as soon as a verification query returns 1. The nonce-respecting MAC advantage of $\mathcal{A}$ and the nonce-respecting (q, v) -MAC advantage of $\mathcal{A}$ are defined by

$$\text{Adv}_{\text{MAC}}^{\text{mac}}(\mathcal{A}) := \Pr[\mathcal{A}^{\text{Tag}_K, \text{Vrfy}_K} \text{ succeeds}], \quad \text{Adv}_{\text{MAC}}^{\text{mac}}(q, v) := \max_{\mathcal{A}} \text{Adv}_{\text{MAC}}^{\text{mac}}(\mathcal{A}),$$

where the maximum ranges over all deterministic, adaptive, nonce-respecting (q, v) -adversaries. Randomized adversaries cannot increase this quantity, because one may condition on their coins.

We consider $1 \leq q < 2^n$ and $v \geq 1$. The maximum defining the MAC advantage is unchanged if we restrict to adversaries making exactly q authentication queries and exactly v verification queries. Any adversary making fewer queries can be padded with additional authentication queries on unused nonces and additional fresh verification queries, without decreasing its success probability. Hence, below we consider only such MAC adversaries.

2.3 Tools: Distance, permutation, and reusable estimates

For probability distributions P, Q on the same finite set Ω , define their statistical distance, Hellinger distance, χ^2 divergence, and KL divergence by

$$\begin{aligned}\Delta(P, Q) &:= \frac{1}{2} \sum_x |P(x) - Q(x)|, \\ H(P, Q) &:= \left(\sum_x (\sqrt{P(x)} - \sqrt{Q(x)})^2 \right)^{1/2}, \\ \chi^2(P\|Q) &:= \sum_x \frac{(P(x) - Q(x))^2}{Q(x)}, \\ D_{\text{KL}}(P\|Q) &:= \sum_x P(x) \log \frac{P(x)}{Q(x)}.\end{aligned}$$

All logarithms are natural. In the last two definitions, a summand with $P(x) = Q(x) = 0$ is zero, while the divergence is $+\infty$ if $P(x) > 0 = Q(x)$ for some x . For KL divergence, every summand with $P(x) = 0$ is interpreted as zero. Write $P \ll Q$ when $Q(x) = 0$ implies $P(x) = 0$. For a function $f : \Omega \rightarrow \Omega'$ into a finite set Ω' , write $f_{\#}P$ for the push-forward distribution, namely $(f_{\#}P)(y) := \sum_{x: f(x)=y} P(x)$.

Proposition 1 (Standard divergence facts). *Let P, Q be probability distributions on a finite set Ω , and let Ω' be a finite set.*

(i) *One always has $\Delta(P, Q) \leq H(P, Q)$. If $P \ll Q$, then*

$$\begin{aligned}H^2(P, Q) &\leq \chi^2(P\|Q), & D_{\text{KL}}(P\|Q) &\leq \chi^2(P\|Q), \\ \Delta(P, Q) &\leq \sqrt{\frac{D_{\text{KL}}(P\|Q)}{2}}.\end{aligned}$$

(ii) *Data processing. For every function $f : \Omega \rightarrow \Omega'$,*

$$\Delta(f_{\#}P, f_{\#}Q) \leq \Delta(P, Q), \quad H(f_{\#}P, f_{\#}Q) \leq H(P, Q). \quad (6)$$

If $P \ll Q$, then $f_{\#}P \ll f_{\#}Q$ and $D_{\text{KL}}(f_{\#}P\|f_{\#}Q) \leq D_{\text{KL}}(P\|Q)$.

(iii) *KL chain rule. Let $P_{X,Y}, Q_{X,Y}$ be joint distributions on a finite set $\mathcal{X} \times \mathcal{Y}$. Suppose $P_X \ll Q_X$ and, for every x with $P_X(x) > 0$, $P_{Y|X=x} \ll Q_{Y|X=x}$. Then*

$$D_{\text{KL}}(P_{X,Y}\|Q_{X,Y}) = D_{\text{KL}}(P_X\|Q_X) + \sum_{x \in \mathcal{X}} P_X(x) D_{\text{KL}}(P_{Y|X=x}\|Q_{Y|X=x}).$$

Terms with $P_X(x) = 0$ are zero.

Proofs of these classical facts can be found in [9,10,17].

We also use the decomposition of squared Hellinger distance. In the next identity, ω_t denotes the complete history retained through time t , P_t, Q_t are its laws, and $P_{t+1|\omega_t}, Q_{t+1|\omega_t}$ are the conditional next-state laws. Conditional laws at histories having zero weight under either law may be chosen arbitrarily. Then

$$H^2(P_{0:q}, Q_{0:q}) = H^2(P_0, Q_0) + \sum_{t=0}^{q-1} \sum_{\omega_t} \sqrt{P_t(\omega_t)Q_t(\omega_t)} H^2(P_{t+1|\omega_t}, Q_{t+1|\omega_t}). \quad (7)$$

For a joint variable (J, T) , the same decomposition gives

$$H^2(P_{J,T}, Q_{J,T}) = H^2(P_J, Q_J) + \sum_j \sqrt{P_J(j)Q_J(j)} H^2(P_{T|j}, Q_{T|j}). \quad (8)$$

Recall a standard fact about random permutations that will be intensively used: after conditioning a random permutation on k distinct input/output pairs, its restriction to the two complements is a uniform bijection. In particular, the image of a new input is uniform over the $2^n - k$ unused outputs.

We present a lemma used in the EWC and EWCDMD analyses. For any sequence $Z_1, \dots, Z_q$ and every $t \in [q]$, partition $[t]$ according to equality among $Z_1, \dots, Z_t$, denote the block sizes by $s_1, \dots, s_r$, and define

$$\xi_t(Z) := \max_{\alpha} s_{\alpha}, \quad \Psi_t(Z) := \sum_{\alpha: s_{\alpha} \geq 2} s_{\alpha}^2.$$

Lemma 1. *Let $Z_1, \dots, Z_q$ be random variables taking values in a finite set $\mathcal{Z}$. For each $i \in [q]$, let H_{i-1} be a finite-valued random variable determining $Z_1, \dots, Z_{i-1}$. Suppose that, for some $D > 0$, every $i \in [q]$, every h_{i-1} with $\Pr[H_{i-1} = h_{i-1}] > 0$, and every $z \in \mathcal{Z}$ satisfy*

$$\Pr[Z_i = z \mid H_{i-1} = h_{i-1}] \leq D^{-1}.$$

Then the following hold.

(i) *For any pairwise disjoint nonempty sets $I_1, \dots, I_s \subseteq [q]$,*

$$\Pr[Z_i = Z_j \text{ for all } i, j \in I_{\ell}, \ell \in [s]] \leq D^{-\sum_{\ell=1}^s (|I_{\ell}|-1)}. \quad (9)$$

(ii) *For every $t \in [q]$,*

$$\mathbb{E}[\Psi_t(Z)] \leq \frac{2t^2}{D}, \quad \mathbb{E}[\Psi_t^2(Z)] \leq \frac{8t^2}{D} + \frac{4t^4}{D^2}.$$

(iii) *For every integer $L \geq 1$,*

$$\Pr[\xi_q(Z) > L] \leq \binom{q}{L+1} D^{-L}.$$

Proof. (i) Let

$$m := \sum_{\ell=1}^s (|I_\ell| - 1).$$

We prove the claim by induction on m . If $m = 0$, then every I_ℓ is a singleton, so the claimed event is certain and the bound is immediate.

Now assume $m \geq 1$. Singleton sets impose no restriction and may be omitted. Let

$$j := \max_{\ell=1}^s I_\ell.$$

After relabeling the sets if necessary, suppose that $j \in I_s$, and put

$$i := \min I_s, \quad I'_s := I_s \setminus \{j\}.$$

Let E denote the event in Equation (9), and let E' be the analogous event with I_s replaced by I'_s . Since $|I_s| \geq 2$, the set I'_s is nonempty, and

$$E = E' \cap \{Z_j = Z_i\}.$$

By the maximality of j , the event E' and the variable Z_i are determined by H_{j-1} . For every h with $\Pr[H_{j-1} = h] > 0$, let z_h be the value of Z_i determined by $H_{j-1} = h$. Then

$$\Pr[Z_j = Z_i \mid H_{j-1} = h] = \Pr[Z_j = z_h \mid H_{j-1} = h] \leq D^{-1}.$$

Consequently,

$$\begin{aligned} \Pr[E] &= \mathbb{E}[\mathbf{1}_{E'} \Pr[Z_j = Z_i \mid H_{j-1}]] \\ &\leq D^{-1} \Pr[E']. \end{aligned}$$

Replacing I_s by I'_s reduces m by one. Hence the induction hypothesis gives

$$\Pr[E'] \leq D^{-(m-1)},$$

and therefore

$$\Pr[E] \leq D^{-m} = D^{-\sum_{\ell=1}^s (|I_\ell| - 1)}.$$

This proves Equation (9).

(ii) Let

$$C_t := \sum_{1 \leq i < j \leq t} \mathbf{1}_{\{Z_i = Z_j\}}.$$

An equality block of size $b \geq 2$ contributes b^2 to $\Psi_t(Z)$ and $\binom{b}{2}$ to C_t . Since $b^2 \leq 4\binom{b}{2}$, we have $\Psi_t(Z) \leq 4C_t$. By (i),

$$\mathbb{E}[C_t] \leq \binom{t}{2} D^{-1},$$

and hence

$$\mathbb{E}[\Psi_t(Z)] \leq 4 \binom{t}{2} D^{-1} \leq \frac{2t^2}{D}.$$

Expanding C_t^2 , each diagonal term has expectation at most D^{-1} , while any two distinct pair equalities have joint probability at most D^{-2} by (i): apply it either to two disjoint pairs or to their three-position union. Therefore,

$$\mathbb{E}[C_t^2] \leq \frac{\binom{t}{2}}{D} + 2 \binom{\binom{t}{2}}{2} \frac{1}{D^2} \leq \frac{t^2}{2D} + \frac{t^4}{4D^2}.$$

Using $\Psi_t(Z) \leq 4C_t$ yields

$$\mathbb{E}[\Psi_t^2(Z)] \leq 16\mathbb{E}[C_t^2] \leq \frac{8t^2}{D} + \frac{4t^4}{D^2}.$$

(iii) If $\xi_q(Z) > L$, then some $L+1$ positions carry the same value. Thus, by (i) and a union bound,

$$\Pr[\xi_q(Z) > L] \leq \sum_{\substack{I \subseteq [q] \\ |I|=L+1}} \Pr[Z_i = Z_j \text{ for all } i, j \in I] \leq \binom{q}{L+1} D^{-L}.$$

□

3 List Forgery

We reduce the MAC advantage to the list forgery advantage, at the cost of the probability of a bad event. Such matching events have also been treated separately in MAC analyses, as in the analysis of `bad`₄ by Choi et al. [4, Sect. 6.1].

List forgery advantage. In the list forgery experiment, a computationally unbounded deterministic adversary $\mathcal{D}$ makes exactly q adaptive authentication queries with distinct nonces. Starting with $Q_0 := \emptyset$, query i is determined by Q_{i-1} , and the answer $T_i := \text{MAC}_K(N_i, M_i)$ gives the transcript

$$Q_i := ((N_1, M_1, T_1), \dots, (N_i, M_i, T_i)).$$

After receiving Q_q , the adversary outputs a list of v verification candidates

$$\mathcal{V}(Q_q) := ((N'_1, M'_1, T'_1), \dots, (N'_v, M'_v, T'_v))$$

satisfying the triple freshness condition

$$(N'_j, M'_j, T'_j) \neq (N_i, M_i, T_i) \quad \text{for all } i \in [q], j \in [v]. \quad (10)$$

Write `Real` for this experiment and define the event

$$\text{Forge}_{\text{MAC}}^{\mathcal{D}} := \{\exists j \in [v] : T'_j = \text{MAC}_K(N'_j, M'_j)\}.$$

The list forgery advantage of $\mathcal{D}$ and the (q, v) -list forgery advantage of MAC are

$$\begin{aligned}\text{Adv}_{\text{MAC}}^{\text{list-forg}}(\mathcal{D}) &:= \Pr_{\text{Real}}[\text{Forge}_{\text{MAC}}^{\mathcal{D}}], \\ \text{Adv}_{\text{MAC}}^{\text{list-forg}}(q, v) &:= \max_{\mathcal{D}} \text{Adv}_{\text{MAC}}^{\text{list-forg}}(\mathcal{D}),\end{aligned}$$

where the maximum is taken over all $\mathcal{D}$ satisfying the preceding conditions. We abbreviate the forgery event to **Forge** when unambiguous.

Strengthening the triple freshness condition to pair freshness

$$(N'_j, M'_j) \neq (N_i, M_i) \quad \text{for all } i \in [q], j \in [v] \quad (11)$$

does not change the maximum advantage. Pair freshness implies triple freshness. Conversely, from any triple-fresh adversary $\mathcal{D}$, construct a pair-fresh adversary $\mathcal{D}'$ by replacing every output candidate whose pair occurs in Q_q with an arbitrary pair-fresh candidate. Any candidate whose pair occurs in Q_q is necessarily rejected. Hence $\mathcal{D}'$ has advantage at least that of $\mathcal{D}$.

Reduction to list forgery. Define an auxiliary experiment **MacRej** by replacing Vrfy_K in the MAC experiment of Section 2.2 with **Rej**, which returns 0 to every verification query without evaluating the MAC. For a (q, v) -adversary $\mathcal{A}$ as in Section 2.2, define

$$\text{Bad}_{\text{MAC}}^{\mathcal{A}} := \{\exists i \in [q], j \in [v] : (N_i, M_i, T_i) = (N'_j, M'_j, T'_j)\}.$$

By Equation (5), any such match has $i > t_j$. Define

$$\delta_{\text{MAC}}(q, v) := \max_{\mathcal{A}} \Pr_{\text{MacRej}}[\text{Bad}_{\text{MAC}}^{\mathcal{A}}],$$

where the maximum is taken over all such $\mathcal{A}$.

Proposition 2. For $1 \leq q < 2^n$ and $v \geq 1$,

$$\text{Adv}_{\text{MAC}}^{\text{mac}}(q, v) \leq \text{Adv}_{\text{MAC}}^{\text{list-forg}}(q, v) + \delta_{\text{MAC}}(q, v). \quad (12)$$

Proof. Fix a (q, v) -adversary $\mathcal{A}$ in the MAC experiment of Section 2.2. Construct a list-forgery adversary $\mathcal{B}$ that runs $\mathcal{A}$, forwards its authentication queries, and answers every verification query with 0, thereby simulating **MacRej**. Write

$$Q_q^{\text{MacRej}} := ((N_i, M_i, T_i))_{i \in [q]}, \quad \mathcal{V}_v^{\text{MacRej}} := ((N'_j, M'_j, T'_j, 0))_{j \in [v]}$$

for the transcripts obtained in this simulation. After the interaction, $\mathcal{B}$ chooses a nonce N^* not used in Q_q^{MacRej} , and submits its verification list $((N''_j, M'_j, T'_j))_{j \in [v]}$, where $N''_j := N^*$ if $(N'_j, M'_j, T'_j) = (N_i, M_i, T_i)$ for some $i \in [q]$, and $N''_j := N'_j$ otherwise. Then the list satisfies Equation (10).

Run the MAC experiment of $\mathcal{A}$ and the list-forgery experiment of $\mathcal{B}$ using the same key K . If $\mathcal{A}$ succeeds, consider its first accepted verification triple. All preceding verification replies are 0, so the simulation inside $\mathcal{B}$ records the

same query triple in $\mathcal{V}_v^{\text{MacRej}}$. If this triple does not occur in Q_q^{MacRej} , it remains unchanged in $\mathcal{B}$'s output list and $\mathcal{B}$ succeeds. Otherwise, $\text{Bad}_{\text{MAC}}^A$ occurs. Hence, pointwise,

$$\mathbf{1}_{\{\mathcal{A} \text{ succeeds}\}} \leq \mathbf{1}_{\{\mathcal{B} \text{ succeeds}\}} + \mathbf{1}_{\{\text{Bad}_{\text{MAC}}^A\}}.$$

Taking expectations over K gives

$$\text{Adv}_{\text{MAC}}^{\text{mac}}(\mathcal{A}) \leq \text{Adv}_{\text{MAC}}^{\text{list-forge}}(\mathcal{B}) + \Pr_{\text{MacRej}}[\text{Bad}_{\text{MAC}}^A].$$

Finally, $\text{Adv}_{\text{MAC}}^{\text{list-forge}}(\mathcal{B}) \leq \text{Adv}_{\text{MAC}}^{\text{list-forge}}(q, v)$, and maximizing over $\mathcal{A}$ proves Equation (12). $\square$

Lemma 2. For $1 \leq q < 2^n$ and $v \geq 1$,

$$\delta_{\text{EWC}}(q, v) \leq \frac{v}{2^n - q + 1}, \quad (13)$$

$$\delta_{\text{EWCDMD}}(q, v) \leq \frac{(n+1)v}{2^n - q + 1}. \quad (14)$$

Proof. Fix $\text{MAC} \in \{\text{EWC}, \text{EWCDMD}\}$ and an adversary $\mathcal{A}$ as in Section 2.2, and work in MacRej . For $i \in [q]$, let Bad_i be the event that the i -th authentication record (N_i, M_i, T_i) coincides with a preceding verification candidate. By its definition,

$$\text{Bad}_{\text{MAC}}^A \subseteq \bigcup_{i=1}^q \text{Bad}_i.$$

Let $Q_{<i}$ be the transcript before the i -th authentication query, and let k_i count preceding verification candidates with input pair (N_i, M_i) . Since authentication nonces are distinct, fixing a complete transcript Q , we have $\sum_{i=1}^q k_i \leq v$.

For EWC, fix $i \in [q]$ and condition on any positive-probability $(Q_{<i}, h, P_2)$. Then (N_i, M_i) and the $i-1$ previously used outputs of P_1 are fixed, and $P_1(N_i)$ is uniform over the remaining $2^n - i + 1$ outputs. Since $x \mapsto P_2(x \oplus h(M_i))$ is a bijection,

$$\Pr_{\text{MacRej}}[\text{Bad}_i \mid Q_{<i}, h, P_2] \leq \frac{k_i}{2^n - i + 1}.$$

Averaging over h, P_2 gives

$$\Pr_{\text{MacRej}}[\text{Bad}_i \mid Q_{<i}] \leq \frac{k_i}{2^n - i + 1}.$$

Hence, by a union bound,

$$\begin{aligned} \Pr_{\text{MacRej}}[\text{Bad}_{\text{EWC}}^A] &\leq \sum_{i=1}^q \Pr_{\text{MacRej}}[\text{Bad}_i] \\ &\leq \sum_{i=1}^q \mathbb{E}_{\text{MacRej}} \left[\frac{k_i}{2^n - i + 1} \right] \\ &\leq \frac{1}{2^n - q + 1} \mathbb{E}_{\text{MacRej}} \left[\sum_{i=1}^q k_i \right] \leq \frac{v}{2^n - q + 1}. \end{aligned}$$

Maximizing over $\mathcal{A}$ proves Equation (13).

For EWCDMD, $\theta \in \mathbb{F}_2^n$, and a fixed permutation P_2 , define

$$\kappa_\theta := |\{x \in \mathbb{F}_2^n : P_2(x) \oplus x = \theta\}|, \quad \kappa_{\max}(P_2) := \max_\theta \kappa_\theta.$$

Fix $i \in [q]$ and condition on any positive-probability $(Q_{<i}, h, P_2)$. After further conditioning on the outputs of P_1 at the preceding authentication nonces, the value $P_1(N_i)$ is uniform over the $2^n - i + 1$ unused outputs. Writing $x := P_1(N_i)$, the EWCDMD tag is $P_2(x \oplus h(M_i)) \oplus x \oplus h(M_i)$. So each fixed tag value has at most $\kappa_{\max}(P_2)$ preimages in x . Hence the conditional probability of Bad_i is at most $k_i \kappa_{\max}(P_2) / (2^n - i + 1)$. Averaging over h and the preceding outputs of P_1 gives

$$\Pr_{\text{MacRej}}[\text{Bad}_i \mid Q_{<i}, P_2] \leq \frac{k_i \kappa_{\max}(P_2)}{2^n - i + 1}.$$

Hence, by a union bound,

$$\begin{aligned} \Pr_{\text{MacRej}}[\text{Bad}_{\text{MAC}}^{\mathcal{A}}] &\leq \sum_{i=1}^q \Pr_{\text{MacRej}}[\text{Bad}_i] \\ &\leq \sum_{i=1}^q \mathbb{E}_{\text{MacRej}} \left[\frac{k_i \kappa_{\max}(P_2)}{2^n - i + 1} \right] \\ &\leq \frac{v \mathbb{E}_{P_2}[\kappa_{\max}(P_2)]}{2^n - q + 1}. \end{aligned}$$

It remains to bound $\mathbb{E}_{P_2}[\kappa_{\max}(P_2)]$ for uniform P_2 . Fix $\theta \in \mathbb{F}_2^n$ and $1 \leq s \leq 2^n$. By definition,

$$\binom{\kappa_\theta}{s} = \sum_{\substack{S \subseteq \mathbb{F}_2^n \\ |S|=s}} \mathbf{1}\{P_2(x) = x \oplus \theta \text{ for all } x \in S\}.$$

Hence we have

$$\mathbb{E}_{P_2} \binom{\kappa_\theta}{s} = \sum_{\substack{S \subseteq \mathbb{F}_2^n \\ |S|=s}} \Pr[P_2(x) = x \oplus \theta \text{ for all } x \in S] = \binom{2^n}{s} \frac{1}{(2^n)_s} = \frac{1}{s!}.$$

Next, it holds that

$$\kappa_{\max}(P_2) \leq n + \sum_{\theta \in \mathbb{F}_2^n} \max\{0, \kappa_\theta - n\} \leq n + \sum_{\theta \in \mathbb{F}_2^n} \binom{\kappa_\theta}{n+1}.$$

Taking expectations and applying the preceding identity with $s = n + 1$ gives

$$\mathbb{E}_{P_2}[\kappa_{\max}(P_2)] \leq n + \sum_{\theta \in \mathbb{F}_2^n} \mathbb{E}_{P_2} \binom{\kappa_\theta}{n+1} = n + \frac{2^n}{(n+1)!} \leq n + 1.$$

Substituting this estimate and maximizing over $\mathcal{A}$ proves Equation (14). $\square$

4 Security of EWC

The main result of this section is as follows.

Theorem 1. *If $1 \leq q \leq 2^n/24$, then*

$$\text{Adv}_{\text{EWC}}^{\text{mac}}(q, v) \leq \frac{4v}{2^n} + v\varepsilon + \frac{q^2\varepsilon}{2 \cdot 2^n} + \frac{q^6}{240 \cdot 2^{5n}} + \frac{2q}{2^{3n/2}} + \frac{5q^2}{2^{2n}} + \frac{8q^3}{2^{5n/2}}. \quad (15)$$

By Proposition 2 and Lemma 2, it remains to bound the list forgery advantage. Fix a deterministic, adaptive, nonce-respecting adversary $\mathcal{D}$ satisfying Equation (11), and let **Real** denote the list forgery experiment of Section 3 instantiated with EWC.

We split the forgery event according to the source of randomness used in its analysis. For a repeated nonce with a previously authenticated tag, injectivity of P_2 reduces acceptance to a hash coincidence, handled via the **Real-Clr-Msg** comparison introduced later and the AXU property. This will be formalized as an event **Copy_{EWC}** below. For a repeated nonce with a different tag, acceptance is controlled by the residual randomness of P_2 , while for a new nonce it is controlled by the residual randomness of P_1 . The latter two cases will be formalized as events **NC_{EWC}** and **NN_{EWC}**, respectively:

$$\begin{aligned} \text{Copy}_{\text{EWC}} &:= \{\exists i \in [q], j \in [v] : N'_j = N_i, T'_j = T_i, h(M'_j) = h(M_i)\}, \\ \text{NC}_{\text{EWC}} &:= \left\{ \exists i \in [q], j \in [v] : \begin{array}{l} N'_j = N_i, T'_j \neq T_i, \\ P_2^{-1}(T'_j) \oplus h(M'_j) = P_2^{-1}(T_i) \oplus h(M_i) \end{array} \right\}, \\ \text{NN}_{\text{EWC}} &:= \{\exists j \in [v] : N'_j \notin \{N_1, \dots, N_q\}, T'_j = P_2(P_1(N'_j) \oplus h(M'_j))\}. \end{aligned}$$

In **Real**, by the definition of **Forge**, we have

$$\text{Forge} = \text{Copy}_{\text{EWC}} \cup \text{NC}_{\text{EWC}} \cup \text{NN}_{\text{EWC}}.$$

Hence,

$$\Pr_{\text{Real}}[\text{Forge}] \leq \Pr_{\text{Real}}[\text{Copy}_{\text{EWC}}] + \Pr_{\text{Real}}[\text{NC}_{\text{EWC}}] + \Pr_{\text{Real}}[\text{NN}_{\text{EWC}}]. \quad (16)$$

In Section 4.1, we bound the probabilities of **NN_{EWC}** and **NC_{EWC}** in **Real**. For **Copy_{EWC}**, we introduce the auxiliary experiments **Clr** and **Msg** in Section 4.2, where we bound the probability of **Copy_{EWC}** in **Msg** and the statistical distance between the joint (h, Q_q) distributions in **Msg** and **Clr**. We bound a conditional divergence χ_t^2 for **Real** and **Clr** in Section 4.3, then use the KL chain rule and a stopped KL argument in Section 4.4 to bound the corresponding statistical distance between **Real** and **Clr**. The estimates are assembled in Section 4.5 to obtain the MAC security bound.

For authentication query i , put $Y_i := P_1(N_i) \oplus h(M_i)$. We call $h(M_i)$ the color of query i and Y_i its root.

4.1 New-nonce and non-copy repeated-nonce forgeries

Proposition 3. *If $q < 2^n$, then*

$$\Pr_{\text{Real}}[\text{NN}_{\text{EWC}}] \leq \frac{v}{2^n - q}. \quad (17)$$

Proof. Fix a value (h, Q_q, P_2) having positive probability in **Real**; it determines the verification list. The transcript fixes q input-output pairs of P_1 . At a new nonce, the residual output is uniform among $2^n - q$ values, and acceptance specifies at most one of them. Therefore, a union bound over the new-nonce verification candidates gives

$$\Pr_{\text{Real}}[\text{NN}_{\text{EWC}} \mid h, Q_q, P_2] \leq \frac{v}{2^n - q}.$$

Averaging gives (17). $\square$

To bound $\Pr_{\text{Real}}[\text{NC}_{\text{EWC}}]$, we first control the tag multiplicities and the conditional roots in **Real**. Fix $t \in [q]$, $h \in \mathcal{H}$, and an authentication transcript

$$Q_t = ((N_i, M_i, T_i))_{i=1}^t.$$

Partition $[t]$ by equal tags. Let $\theta_1, \dots, \theta_r$ be the distinct values among $T_1, \dots, T_t$, with

$$I_\alpha := \{i \in [t] : T_i = \theta_\alpha\}, \quad s_\alpha := |I_\alpha|, \quad C_\alpha := \{h(M_i) : i \in I_\alpha\}.$$

For $\alpha \in [r]$, let $Y_{(\alpha)} := P_2^{-1}(\theta_\alpha)$ be the root of I_α , so that $Y_i = Y_{(\alpha)}$ for $i \in I_\alpha$. For roots, subscripts i and (α) index queries and blocks, respectively. If $\Pr_{\text{Real}}[Q_t = Q_t, \mathbf{h} = h] > 0$, then $|C_\alpha| = s_\alpha$ for every $\alpha \in [r]$. Indeed, if distinct $i, j \in I_\alpha$ satisfied $h(M_i) = h(M_j)$, then $P_1(N_i) = Y_{(\alpha)} \oplus h(M_i) = Y_{(\alpha)} \oplus h(M_j) = P_1(N_j)$, contradicting $N_i \neq N_j$.

Write $\alpha(i) := \alpha$ for $i \in I_\alpha$ and define the configuration $\mathcal{C} := (C_1, \dots, C_r)$. Set $\xi_0 := 0$ and $\Psi_0 := 0$ and, for $t \geq 1$, put

$$\xi_t := \max_{\alpha} s_\alpha, \quad \Psi_t := \sum_{\alpha: s_\alpha \geq 2} s_\alpha^2.$$

Lemma 3. *Assume $q < 2^n$. For $0 \leq t \leq q$ and any integer $L \geq 1$,*

$$\mathbb{E}_{\text{Real}}[\Psi_t] \leq \frac{2t^2}{2^n - q}, \quad \mathbb{E}_{\text{Real}}[\Psi_t^2] \leq \frac{8t^2}{2^n - q} + \frac{4t^4}{(2^n - q)^2}, \quad (18)$$

$$\Pr_{\text{Real}}[\xi_q > L] \leq \binom{q}{L+1} (2^n - q)^{-L}. \quad (19)$$

Proof. Fix $i \in [q]$ and a tag θ , and condition on a positive-probability value of $H_{i-1} := (h, P_2, Q_{i-1})$ in **Real**. The fresh P_1 output is uniform on $2^n - i + 1$ values, while $T_i = \theta$ specifies at most one of them. Hence

$$\Pr_{\text{Real}}[T_i = \theta \mid H_{i-1}] \leq \frac{1}{2^n - q}.$$

Apply Lemma 1 with $Z_i = T_i$ and $D = 2^n - q$. $\square$

We next describe the conditional root distribution. Define

$$\mathfrak{P}(\mathcal{C}) := \left\{ (y_{(1)}, \dots, y_{(r)}) \in (\mathbb{F}_2^n)^r : \begin{array}{l} y_{(\alpha)} \neq y_{(\beta)}, \\ (y_{(\alpha)} \oplus C_\alpha) \cap (y_{(\beta)} \oplus C_\beta) = \emptyset \\ \text{for all } \alpha \neq \beta \end{array} \right\}, \quad (20)$$

and let $\text{Pack}(\mathcal{C}) := |\mathfrak{P}(\mathcal{C})|$.

Proposition 4. *Fix values h, Q_t such that $\Pr_{\text{Real}}[\mathbf{Q}_t = Q_t, \mathbf{h} = h] > 0$. Then*

$$\Pr_{\text{Real}}[\mathbf{Q}_t = Q_t \mid h] = \frac{\text{Pack}(\mathcal{C})}{(2^n)_t (2^n)_r}.$$

Conditional on h, Q_t , $(Y_{(\alpha)})_{\alpha \in [r]}$ is uniform on $\mathfrak{P}(\mathcal{C})$. Moreover, for every $\beta \in [r]$, after further conditioning on any value of the other roots having positive conditional probability, $Y_{(\beta)}$ is uniform on its conditional support, whose size is at least

$$2^n - (r-1) - s_\beta(t - s_\beta).$$

If $\xi_t \leq L$, this size is at least $2^n - (t-1) - Lt$.

Proof. For $y = (y_{(1)}, \dots, y_{(r)}) \in \mathfrak{P}(\mathcal{C})$, define $\mathcal{E}_y^{h, Q_t}$ as the event

$$P_2(y_{(\alpha)}) = \theta_\alpha \quad (\alpha \in [r]), \quad P_1(N_i) = y_{(\alpha(i))} \oplus h(M_i) \quad (i \in [t]).$$

The P_2 constraints are valid since the values $y_{(\alpha)}$ and θ_α are pairwise distinct. For P_1 , the inputs are distinct because $\mathcal{D}$ is nonce-respecting, while the prescribed outputs are distinct within each block by $|C_\alpha| = s_\alpha$ and across blocks by (20).

Since $\mathcal{D}$ is deterministic, any pair (P_1, P_2) satisfying $\mathcal{E}_y^{h, Q_t}$ produces the transcript Q_t . Conversely, any pair producing Q_t determines the unique root tuple $y = (P_2^{-1}(\theta_1), \dots, P_2^{-1}(\theta_r)) \in \mathfrak{P}(\mathcal{C})$. Hence, conditional on h ,

$$\{\mathbf{Q}_t = Q_t\} = \bigsqcup_{y \in \mathfrak{P}(\mathcal{C})} \mathcal{E}_y^{h, Q_t}, \quad \Pr_{\text{Real}}[\mathcal{E}_y^{h, Q_t} \mid h] = \frac{1}{(2^n)_t (2^n)_r}.$$

It follows that

$$\begin{aligned} \Pr_{\text{Real}}[\mathbf{Q}_t = Q_t \mid h] &= \frac{\text{Pack}(\mathcal{C})}{(2^n)_t (2^n)_r}, \\ \Pr_{\text{Real}}[(Y_{(\alpha)})_{\alpha \in [r]} = y \mid h, Q_t] &= \frac{1}{\text{Pack}(\mathcal{C})} \quad (y \in \mathfrak{P}(\mathcal{C})). \end{aligned} \quad (21)$$

Now fix $\beta \in [r]$ and a value $y_{-\beta} = (y_{(\gamma)})_{\gamma \neq \beta}$ having positive conditional probability. The conditional support of $Y_{(\beta)}$ is

$$\mathcal{S}_\beta(y_{-\beta}) := \mathbb{F}_2^n \setminus (\{y_{(\gamma)} : \gamma \neq \beta\} \cup \{y_{(\gamma)} \oplus c' \oplus c : \gamma \neq \beta, c \in C_\beta, c' \in C_\gamma\}).$$

By (21), $Y_{(\beta)}$ is uniform on $\mathcal{S}_\beta(y_{-\beta})$, and

$$|\mathcal{S}_\beta(y_{-\beta})| \geq 2^n - (r-1) - |C_\beta| \sum_{\gamma \neq \beta} |C_\gamma| = 2^n - (r-1) - s_\beta(t - s_\beta).$$

If $\xi_t \leq L$, then $s_\beta(t - s_\beta) \leq Lt$. Together with $r-1 \leq t-1$, this yields the final bound. $\square$

Proposition 5. *Let $L \geq 1$ be an integer and $q \geq 1$. If $(L+1)q \leq 2^n/4$, then*

$$\Pr_{\text{Real}}[\text{NC}_{\text{EWC}} \cap \{\xi_q \leq L\}] \leq \frac{v}{2^n - (L+1)q + 1}. \quad (22)$$

Proof. Fix (h, Q_q) such that $\Pr_{\text{Real}}[\mathbf{h} = h, \mathbf{Q}_q = Q_q] > 0$ and $\xi_q \leq L$. The verification list is then fixed. For $j \in [v]$, define

$$\mathcal{E}_j := \{\exists i \in [q] : N'_j = N_i, T'_j \neq T_i, P_2^{-1}(T'_j) = Y_i \oplus h(M_i) \oplus h(M'_j)\}.$$

Thus $\text{NC}_{\text{EWC}} = \bigcup_{j=1}^v \mathcal{E}_j$. If no i satisfies the first two conditions defining $\mathcal{E}_j$, then $\mathcal{E}_j$ is empty. Otherwise the nonce condition determines a unique $i \in [q]$.

Suppose first that $T'_j \notin \{\theta_1, \dots, \theta_r\}$. Fix a value y of the root tuple having positive conditional probability. Given $(Y_{(\gamma)})_{\gamma \in [r]} = y$, the value $P_2^{-1}(T'_j)$ is uniform over the $2^n - r$ inputs not mapped to the observed tags. Consequently,

$$\begin{aligned} \Pr_{\text{Real}}[\mathcal{E}_j \mid h, Q_q, (Y_{(\gamma)})_{\gamma \in [r]} = y] &\leq \frac{1}{2^n - r}, \\ \Pr_{\text{Real}}[\mathcal{E}_j \mid h, Q_q] &\leq \frac{1}{2^n - r} \leq \frac{1}{2^n - (L+1)q + 1}, \end{aligned}$$

where the first inequality on the second line follows by averaging over the root tuple.

Now suppose that $T'_j = \theta_\beta$ and $i \in I_\alpha$. Since $T_i = \theta_\alpha \neq T'_j$, we have $\beta \neq \alpha$. By Proposition 4, after conditioning on any value $(Y_{(\gamma)})_{\gamma \neq \beta} = y_{-\beta}$ having positive probability, $Y_{(\beta)}$ is uniform over at least $2^n - (q-1) - Lq = 2^n - (L+1)q + 1$ possible values. Since $\alpha \neq \beta$, the event $\mathcal{E}_j$ specifies at most one of these values. Therefore,

$$\begin{aligned} \Pr_{\text{Real}}[\mathcal{E}_j \mid h, Q_q, (Y_{(\gamma)})_{\gamma \neq \beta} = y_{-\beta}] &\leq \frac{1}{2^n - (L+1)q + 1}, \\ \Pr_{\text{Real}}[\mathcal{E}_j \mid h, Q_q] &\leq \frac{1}{2^n - (L+1)q + 1}, \end{aligned}$$

where the second inequality follows by averaging over the other roots.

A union bound gives

$$\begin{aligned} \Pr_{\text{Real}}[\text{NC}_{\text{EWC}} \mid h, Q_q] &\leq \sum_{j=1}^v \Pr_{\text{Real}}[\mathcal{E}_j \mid h, Q_q] \\ &\leq \frac{v}{2^n - (L+1)q + 1}. \end{aligned}$$

Since ξ_q is determined by Q_q , averaging over (h, Q_q) yields

$$\begin{aligned} \Pr_{\text{Real}}[\text{NC}_{\text{EWC}} \cap \{\xi_q \leq L\}] &= \mathbb{E}_{\text{Real}} \left[\mathbf{1}_{\{\xi_q \leq L\}} \Pr_{\text{Real}}[\text{NC}_{\text{EWC}} \mid \mathbf{h}, \mathbf{Q}_q] \right] \\ &\leq \frac{v}{2^n - (L+1)q + 1}. \end{aligned}$$

□

4.2 The copy event and auxiliary experiments

It remains to bound $\Pr_{\text{Real}}[\text{Copy}_{\text{EWC}}]$. This event is determined by (h, Q_q) . We introduce two auxiliary authentication experiments, **Clr** and **Msg**, identical to **Real** except for the authentication oracle. In both experiments, h is sampled as in **Real**. With the sampled functions fixed, the authentication oracle returns T on query (N, M) as follows:

$$\begin{aligned} \text{Clr} : \quad T &:= \Pi_{h(M)}(N), \\ \text{Msg} : \quad T &:= \Pi_M(N). \end{aligned}$$

When an index is encountered for the first time, the corresponding $\Pi_{h(M)}$ or Π_M is sampled as an independent uniform permutation of $\mathbb{F}_2^n$; later queries with the same index reuse it. All these permutations are mutually independent and independent of h .

In **Msg**, transcript generation does not use h , so AXU bounds the copy event after the transcript is fixed. We therefore compare **Msg** with **Clr**, and then compare **Real** with **Clr**. More explicitly, applying the inequality $|\Pr_P[E] - \Pr_Q[E]| \leq \Delta(P, Q)$ twice gives

$$\begin{aligned} \Pr_{\text{Real}}[\text{Copy}_{\text{EWC}}] &\leq \Pr_{\text{Msg}}[\text{Copy}_{\text{EWC}}] + \Delta(\mathcal{L}_{\text{Msg}}(h, Q_q), \mathcal{L}_{\text{Clr}}(h, Q_q)) \\ &\quad + \Delta(\mathcal{L}_{\text{Real}}(h, Q_q), \mathcal{L}_{\text{Clr}}(h, Q_q)). \end{aligned} \quad (23)$$

Proposition 6.

$$\Pr_{\text{Msg}}[\text{Copy}_{\text{EWC}}] \leq v\varepsilon. \quad (24)$$

Proof. Fix Q_q with $\Pr_{\text{Msg}}[Q_q = Q_q] > 0$. It also fixes the verification list. Since Q_q is independent of h in **Msg**, the conditional distribution of h remains uniform over $\mathcal{H}$.

Let

$$J := \{j \in [v] : \exists i \in [q] \text{ such that } (N'_j, T'_j) = (N_i, T_i)\}.$$

Because the authentication nonces are distinct, for every $j \in J$ there is a unique such index i , denoted i_j . Moreover, freshness gives $M'_j \neq M_{i_j}$. Therefore, by the union bound and Equation (1),

$$\begin{aligned} \Pr_{\text{Msg}}[\text{Copy}_{\text{EWC}} \mid Q_q] &\leq \sum_{j \in J} \Pr_{h \leftarrow \mathcal{H}}[h(M'_j) = h(M_{i_j})] \\ &\leq |J|\varepsilon \leq v\varepsilon. \end{aligned}$$

Averaging over Q_q yields (24). $\square$

Proposition 7. Assume $q < 2^n$. Then

$$\Delta(\mathcal{L}_{\text{Msg}}(h, Q_q), \mathcal{L}_{\text{Clr}}(h, Q_q)) \leq \binom{q}{2} \frac{\varepsilon}{2^n}.$$

Proof. Let **Cmp** be the event

$$h(M_s) = h(M_t) \implies T_s \neq T_t \quad (1 \leq s < t \leq q).$$

Fix $h \in \mathcal{H}$ and $Q_q = ((N_i, M_i, T_i))_{i=1}^q$ with $\Pr_{\text{Msg}}[Q_q = Q_q] > 0$, and put

$$k_M := |\{i \in [q] : M_i = M\}|, \quad k_a := |\{i \in [q] : h(M_i) = a\}|.$$

If $(h, Q_q) \in \text{Cmp}$, interpolation of the random permutations gives

$$\begin{aligned} \Pr_{\text{Msg}}[Q_q = Q_q \mid h] &= \prod_{M: k_M > 0} \frac{1}{(2^n)_{k_M}} \\ &\leq \prod_{a: k_a > 0} \frac{1}{(2^n)_{k_a}} = \Pr_{\text{Clr}}[Q_q = Q_q \mid h]. \end{aligned}$$

Moreover, the **Clr** law is supported on **Cmp**, since distinct authentication nonces are distinct inputs to the permutation for each color. Let

$$p_h(Q_q) := \Pr_{\text{Msg}}[Q_q = Q_q \mid h], \quad q_h(Q_q) := \Pr_{\text{Clr}}[Q_q = Q_q \mid h].$$

Since h has the same marginal distribution in both worlds,

$$\begin{aligned} &\Delta(\mathcal{L}_{\text{Msg}}(h, Q_q), \mathcal{L}_{\text{Clr}}(h, Q_q)) \\ &= \sum_{h \in \mathcal{H}} \Pr_{\text{Msg}}[h = h] \sum_{\substack{Q_q: \\ p_h(Q_q) > q_h(Q_q)}} (p_h(Q_q) - q_h(Q_q)) \\ &= \sum_{h \in \mathcal{H}} \Pr_{\text{Msg}}[h = h] \Pr_{\text{Msg}}[\neg \text{Cmp} \mid h] \\ &= \Pr_{\text{Msg}}[\neg \text{Cmp}]. \end{aligned}$$

Fix Q_q with $\Pr_{\text{Msg}}[Q_q = Q_q] > 0$. Since Q_q is independent of h in **Msg**, by the union bound and Equation (1),

$$\Pr_{\text{Msg}}[\neg \text{Cmp} \mid Q_q] \leq \varepsilon \sum_{1 \leq s < t \leq q} \mathbf{1}_{\{M_s \neq M_t, T_s = T_t\}}.$$

Averaging over Q_q gives

$$\Pr_{\text{Msg}}[\neg \text{Cmp}] \leq \varepsilon \sum_{t=1}^q \sum_{s=1}^{t-1} \Pr_{\text{Msg}}[M_s \neq M_t, T_s = T_t].$$

For $t \in [q]$, let

$$\ell_t := |\{s < t : M_s = M_t\}|.$$

Conditional on Q_{t-1} , where Q_{t-1} has positive probability, T_t is uniform over the $2^n - \ell_t$ outputs not previously used for M_t . Hence

$$\sum_{s=1}^{t-1} \Pr_{\text{Msg}}[M_s \neq M_t, T_s = T_t \mid Q_{t-1}] \leq \frac{t-1-\ell_t}{2^n - \ell_t} \leq \frac{t-1}{2^n}.$$

Averaging over Q_{t-1} gives

$$\sum_{s=1}^{t-1} \Pr_{\text{Msg}}[M_s \neq M_t, T_s = T_t] \leq \frac{t-1}{2^n}.$$

Therefore,

$$\Delta(\mathcal{L}_{\text{Msg}}(h, Q_q), \mathcal{L}_{\text{Clr}}(h, Q_q)) = \Pr_{\text{Msg}}[\neg \text{Comp}] \leq \varepsilon \sum_{t=1}^q \frac{t-1}{2^n} = \binom{q}{2} \frac{\varepsilon}{2^n}.$$

□

4.3 Conditional divergence between the Real and Clr experiments

Fix $0 \leq t \leq q$. For a value (h, Q_t) having positive probability in **Real**, distinct nonces of a fixed color have distinct tags, which implies (h, Q_t) has positive probability in **Clr**. Hence we have $\mathcal{L}_{\text{Real}}(h, Q_t) \ll \mathcal{L}_{\text{Clr}}(h, Q_t)$.

In this subsection we fix $0 \leq t < q$ and a value (h, Q_t) having positive probability in **Real**. All conditional laws below are given h, Q_t . For $t = 0$, take $r = 0$ and $\mathcal{C} = \emptyset$. The adversary determines the next query from Q_t . Write

$$a := h(M_{t+1}), \quad m := |\{i \in [t] : h(M_i) = a\}|, \quad \mathcal{I}_a := \{\alpha \in [r] : a \notin C_\alpha\}.$$

For $\alpha \in \mathcal{I}_a$, write $\mathcal{C}^{\alpha, +a}$ for the configuration obtained by adding a to C_α , and set

$$u_\alpha := \frac{\text{Pack}(\mathcal{C}^{\alpha, +a})}{\text{Pack}(\mathcal{C})}, \quad d_\alpha := u_\alpha - \frac{2^n - t}{2^n - m}. \quad (25)$$

Encode the next tag by a variable J : set $J := \alpha$ if $T_{t+1} = \theta_\alpha$, and set $J := \star$ if T_{t+1} is a new tag. The eligible old blocks are precisely the $r - m$ elements of $\mathcal{I}_a$. Let P_J, Q_J be the conditional laws of J in **Real**, **Clr**, respectively, and let P_T, Q_T be the corresponding conditional laws of T_{t+1} .

Lemma 4. For $\alpha \in \mathcal{I}_a$,

$$\begin{aligned} P_J(\alpha) &= \frac{u_\alpha}{2^n - t}, & P_J(\star) &= 1 - \sum_{\alpha \in \mathcal{I}_a} P_J(\alpha), \\ Q_J(\alpha) &= \frac{1}{2^n - m}, & Q_J(\star) &= \frac{2^n - r}{2^n - m}. \end{aligned} \quad (26)$$

Moreover,

$$D_{\text{KL}}(P_T \| Q_T) = D_{\text{KL}}(P_J \| Q_J), \quad \chi^2(P_T \| Q_T) = \chi^2(P_J \| Q_J). \quad (27)$$

Proof. The transcript Q_t fixes the next query (N_{t+1}, M_{t+1}) . For $\tau \in \mathbb{F}_2^n$, let Q_{t+1}^τ be the transcript obtained by appending (N_{t+1}, M_{t+1}, τ) to Q_t .

Fix $\alpha \in \mathcal{I}_a$. The transcript $Q_{t+1}^{\theta_\alpha}$ has $t+1$ interpolation constraints on P_1 and the same r constraints on P_2 as Q_t ; its root configuration is $\mathcal{C}^{\alpha,+a}$. The counting argument in the proof of Proposition 4 therefore gives

$$\begin{aligned} P_J(\alpha) &= \Pr_{\text{Real}}[T_{t+1} = \theta_\alpha \mid h, Q_t] \\ &= \frac{\Pr_{\text{Real}}[Q_{t+1} = Q_{t+1}^{\theta_\alpha} \mid h]}{\Pr_{\text{Real}}[Q_t = Q_t \mid h]} \\ &= \frac{\text{Pack}(\mathcal{C}^{\alpha,+a})/((2^n)_{t+1}(2^n)_r)}{\text{Pack}(\mathcal{C})/((2^n)_t(2^n)_r)} = \frac{u_\alpha}{2^n - t}. \end{aligned}$$

Since $\alpha \notin \mathcal{I}_a$ implies $P_J(\alpha) = 0$, normalization gives the formula for $P_J(\star)$.

In Clr , the color- a permutation has already been evaluated at the m earlier nonces of color a , producing m distinct old tags. Its next output is uniform over the other $2^n - m$ values. Of the r old tags, precisely these m are unavailable and the remaining $r - m$ correspond to $\mathcal{I}_a$. Hence

$$Q_J(\alpha) = \frac{1}{2^n - m} \quad (\alpha \in \mathcal{I}_a), \quad Q_J(\star) = \frac{2^n - m - (r - m)}{2^n - m} = \frac{2^n - r}{2^n - m}.$$

It remains to compare the distributions within the branches. Put

$$\mathcal{U} := \mathbb{F}_2^n \setminus \{\theta_1, \dots, \theta_r\}.$$

For every $\tau \in \mathcal{U}$, the transcript Q_{t+1}^τ has the same new root configuration $\mathcal{C}^{\star,+a} := (C_1, \dots, C_r, \{a\})$, with $t+1$ interpolation constraints on P_1 and $r+1$ interpolation constraints on P_2 . Thus

$$\begin{aligned} P_T(\tau) &= \frac{\Pr_{\text{Real}}[Q_{t+1} = Q_{t+1}^\tau \mid h]}{\Pr_{\text{Real}}[Q_t = Q_t \mid h]} \\ &= \frac{\text{Pack}(\mathcal{C}^{\star,+a})/((2^n)_{t+1}(2^n)_{r+1})}{\text{Pack}(\mathcal{C})/((2^n)_t(2^n)_r)} \\ &= \frac{\text{Pack}(\mathcal{C}^{\star,+a})}{\text{Pack}(\mathcal{C})(2^n - t)(2^n - r)}, \end{aligned}$$

which is independent of τ . Since $|\mathcal{U}| = 2^n - r$ and $\{J = \star\}$ is the disjoint union of the events $\{T_{t+1} = \tau\}$ over $\tau \in \mathcal{U}$, we have

$$P_T(\tau) = \frac{P_J(\star)}{2^n - r} \quad (\tau \in \mathcal{U}).$$

In Clr , each $\tau \in \mathcal{U}$ is an unused output of the color- a permutation, and hence

$$Q_T(\tau) = \frac{1}{2^n - m} = \frac{Q_J(\star)}{2^n - r} \quad (\tau \in \mathcal{U}).$$

Moreover, for every $\alpha \in \mathcal{I}_a$,

$$P_T(\theta_\alpha) = P_J(\alpha), \quad Q_T(\theta_\alpha) = Q_J(\alpha).$$

For $\beta \in [r] \setminus \mathcal{I}_a$, the tag θ_β has already occurred under color a ; the permutation property in either experiment gives

$$P_T(\theta_\beta) = Q_T(\theta_\beta) = 0.$$

Substitution of these point probabilities into the definitions gives

$$\begin{aligned} D_{\text{KL}}(P_T \| Q_T) &= \sum_{\alpha \in \mathcal{I}_a} P_J(\alpha) \log \frac{P_J(\alpha)}{Q_J(\alpha)} + \sum_{\tau \in \mathcal{U}} \frac{P_J(\star)}{2^n - r} \log \frac{P_J(\star)/(2^n - r)}{Q_J(\star)/(2^n - r)} \\ &= \sum_{\alpha \in \mathcal{I}_a} P_J(\alpha) \log \frac{P_J(\alpha)}{Q_J(\alpha)} + P_J(\star) \log \frac{P_J(\star)}{Q_J(\star)} = D_{\text{KL}}(P_J \| Q_J) \end{aligned}$$

and

$$\begin{aligned} \chi^2(P_T \| Q_T) &= \sum_{\alpha \in \mathcal{I}_a} \frac{(P_J(\alpha) - Q_J(\alpha))^2}{Q_J(\alpha)} \\ &\quad + \sum_{\tau \in \mathcal{U}} \frac{(P_J(\star)/(2^n - r) - Q_J(\star)/(2^n - r))^2}{Q_J(\star)/(2^n - r)} \\ &= \sum_{\alpha \in \mathcal{I}_a} \frac{(P_J(\alpha) - Q_J(\alpha))^2}{Q_J(\alpha)} + \frac{(P_J(\star) - Q_J(\star))^2}{Q_J(\star)} = \chi^2(P_J \| Q_J), \end{aligned}$$

which proves Equation (27). $\square$

Lemma 5. *For the conditional laws P_J, Q_J in Equation (26),*

$$\chi^2(P_J \| Q_J) = \frac{2^n - m}{(2^n - t)^2} \left(\sum_{\alpha \in \mathcal{I}_a} d_\alpha^2 + \frac{(\sum_{\alpha \in \mathcal{I}_a} d_\alpha)^2}{2^n - r} \right). \quad (28)$$

Proof. Substituting Equations (25) and (26) into the definition of $\chi^2(P_J \| Q_J)$ gives Equation (28). $\square$

Continue with the fixed values (h, Q_t) , which have positive probability in both worlds, and assume

$$\xi_t \leq L, \quad (L+1)t \leq 2^n/4, \quad (29)$$

and put

$$D_t := 2^n - (L+1)t, \quad \eta_t := \frac{(L+1)t}{D_t}.$$

Thus $D_t \geq 3 \cdot 2^n/4$ and $\eta_t \leq 1/3$.

For $\alpha \in \mathcal{I}_a$, $\beta \in [r] \setminus \{\alpha\}$, and $c \in C_\beta$, define

$$\mathcal{E}_{\alpha, \beta, c} := \{y \in \mathfrak{P}(\mathcal{C}) : y_{(\alpha)} = y_{(\beta)} \oplus a \oplus c\}.$$

Lemma 6. *If $c = a$ or $(C_\alpha \oplus (a \oplus c)) \cap C_\beta \neq \emptyset$, then $\mathcal{E}_{\alpha,\beta,c} = \emptyset$. Otherwise,*

$$\frac{1 - \eta_t}{2^n} \leq \frac{|\mathcal{E}_{\alpha,\beta,c}|}{|\mathfrak{P}(\mathcal{C})|} \leq \frac{1}{D_t}.$$

Proof. If $c = a$, then every $y \in \mathcal{E}_{\alpha,\beta,c}$ would satisfy $y_{(\alpha)} = y_{(\beta)}$, contradicting $y \in \mathfrak{P}(\mathcal{C})$. If $(C_\alpha \oplus (a \oplus c)) \cap C_\beta \neq \emptyset$, choose $x \in C_\alpha$ and put $w := x \oplus a \oplus c \in C_\beta$. Every $y \in \mathcal{E}_{\alpha,\beta,c}$ would satisfy

$$y_{(\alpha)} \oplus x = y_{(\beta)} \oplus a \oplus c \oplus x = y_{(\beta)} \oplus w,$$

contrary to $y \in \mathfrak{P}(\mathcal{C})$. Thus $\mathcal{E}_{\alpha,\beta,c} = \emptyset$.

Assume henceforth that $c \neq a$ and $(C_\alpha \oplus a \oplus c) \cap C_\beta = \emptyset$, and define $\mathcal{C}_{-\alpha} := (C_\gamma)_{\gamma \neq \alpha}$. Since $|\mathfrak{P}(\mathcal{C})| > 0$, we also have $|\mathfrak{P}(\mathcal{C}_{-\alpha})| > 0$. For $z = (z_{(\gamma)})_{\gamma \neq \alpha} \in \mathfrak{P}(\mathcal{C}_{-\alpha})$, write z^{+u} for the full tuple whose α th coordinate is u and whose remaining coordinates are those of z , and put

$$\mathcal{S}(z) := \{u \in \mathbb{F}_2^n : z^{+u} \in \mathfrak{P}(\mathcal{C})\}, \quad \mathcal{G} := \{z \in \mathfrak{P}(\mathcal{C}_{-\alpha}) : z_{(\beta)} \oplus a \oplus c \in \mathcal{S}(z)\}.$$

Deleting the α th coordinate gives

$$|\mathfrak{P}(\mathcal{C})| = \sum_{z \in \mathfrak{P}(\mathcal{C}_{-\alpha})} |\mathcal{S}(z)|, \quad |\mathcal{E}_{\alpha,\beta,c}| = |\mathcal{G}| \leq |\mathfrak{P}(\mathcal{C}_{-\alpha})|. \quad (30)$$

For fixed $z \in \mathfrak{P}(\mathcal{C}_{-\alpha})$, a value u is excluded from $\mathcal{S}(z)$ only if, for some $\gamma \neq \alpha$, either $u = z_{(\gamma)}$ or $u \oplus x = z_{(\gamma)} \oplus w$ for some $x \in C_\alpha$ and $w \in C_\gamma$. Hence

$$|\mathcal{S}(z)| \geq 2^n - (r - 1) - s_\alpha(t - s_\alpha) \geq D_t.$$

It follows from Equation (30) that

$$\frac{|\mathcal{E}_{\alpha,\beta,c}|}{|\mathfrak{P}(\mathcal{C})|} \leq \frac{|\mathfrak{P}(\mathcal{C}_{-\alpha})|}{D_t |\mathfrak{P}(\mathcal{C}_{-\alpha})|} \leq \frac{1}{D_t}.$$

We next record the counting estimate used for the lower bound. For distinct $\rho, \gamma \in [r] \setminus \{\alpha\}$ and $\zeta \in \mathbb{F}_2^n$, let

$$\mathcal{A}_{\rho,\gamma,\zeta} := \{z \in \mathfrak{P}(\mathcal{C}_{-\alpha}) : z_{(\rho)} = z_{(\gamma)} \oplus \zeta\}. \quad (31)$$

Let $\mathcal{C}_{-\alpha,-\rho}$ be obtained by deleting blocks α and ρ . Deleting coordinate ρ maps $\mathcal{A}_{\rho,\gamma,\zeta}$ injectively into $\mathfrak{P}(\mathcal{C}_{-\alpha,-\rho})$. Each tuple in the latter set has at least

$$2^n - (r - 2) - s_\rho(t - s_\alpha - s_\rho) \geq D_t$$

extensions in $\mathfrak{P}(\mathcal{C}_{-\alpha})$. Therefore,

$$|\mathcal{A}_{\rho,\gamma,\zeta}| \leq |\mathfrak{P}(\mathcal{C}_{-\alpha,-\rho})| \leq \frac{|\mathfrak{P}(\mathcal{C}_{-\alpha})|}{D_t}.$$

Because $a \neq c$ and $(C_\alpha \oplus a \oplus c) \cap C_\beta = \emptyset$, a tuple $z \in \mathfrak{P}(\mathcal{C}_{-\alpha}) \setminus \mathcal{G}$ must satisfy, for some $\gamma \notin \{\alpha, \beta\}$,

$$z_{(\beta)} \oplus a \oplus c = z_{(\gamma)} \quad \text{or} \quad z_{(\beta)} \oplus a \oplus c \oplus x = z_{(\gamma)} \oplus w \quad (x \in C_\alpha, w \in C_\gamma).$$

Each equality defines a set of the form in Equation (31). Their number is at most

$$(r-2) + s_\alpha \sum_{\gamma \notin \{\alpha, \beta\}} s_\gamma = (r-2) + s_\alpha(t - s_\alpha - s_\beta) \leq (L+1)t.$$

Thus

$$|\mathfrak{P}(\mathcal{C}_{-\alpha}) \setminus \mathcal{G}| \leq \frac{(L+1)t}{D_t} |\mathfrak{P}(\mathcal{C}_{-\alpha})| = \eta_t |\mathfrak{P}(\mathcal{C}_{-\alpha})|, \quad |\mathcal{G}| \geq (1 - \eta_t) |\mathfrak{P}(\mathcal{C}_{-\alpha})|.$$

Finally, $|\mathcal{S}(z)| \leq 2^n$ for every $z \in \mathfrak{P}(\mathcal{C}_{-\alpha})$, and hence

$$|\mathfrak{P}(\mathcal{C})| = \sum_{z \in \mathfrak{P}(\mathcal{C}_{-\alpha})} |\mathcal{S}(z)| \leq 2^n |\mathfrak{P}(\mathcal{C}_{-\alpha})|.$$

Using Equation (30) once more,

$$\frac{|\mathcal{E}_{\alpha, \beta, c}|}{|\mathfrak{P}(\mathcal{C})|} \geq \frac{(1 - \eta_t) |\mathfrak{P}(\mathcal{C}_{-\alpha})|}{2^n |\mathfrak{P}(\mathcal{C}_{-\alpha})|} = \frac{1 - \eta_t}{2^n}.$$

□

For $\alpha \in \mathcal{I}_a$, define

$$B_\alpha := s_\alpha + |\{(\beta, c) : \beta \in [r] \setminus \{\alpha\}, c \in C_\beta \setminus \{a\}, (C_\alpha \oplus (a \oplus c)) \cap C_\beta \neq \emptyset\}|. \quad (32)$$

Lemma 7. *Let $L \geq 1$. If $\xi_t \leq L$ and $(L+1)t \leq 2^n/4$, then*

$$|d_\alpha| \leq \frac{4B_\alpha}{3 \cdot 2^n} + 2(L+1) \frac{t^2}{2^{2n}} \quad (33)$$

for every $\alpha \in \mathcal{I}_a$, and

$$\sum_{\alpha \in \mathcal{I}_a} B_\alpha^2 \leq 2(t + \Psi_t) + \frac{t}{2} \Psi_t^2. \quad (34)$$

Proof. Fix $\alpha \in \mathcal{I}_a$. Since exactly m blocks of $\mathcal{C}$ contain a and $\sum_{\beta=1}^r s_\beta = t$,

$$|\{(\beta, c) : \beta \in [r] \setminus \{\alpha\}, c \in C_\beta \setminus \{a\}\}| = t - m - s_\alpha.$$

By Equation (32), exactly $B_\alpha - s_\alpha$ of these pairs satisfy $(C_\alpha \oplus (a \oplus c)) \cap C_\beta \neq \emptyset$. Therefore,

$$|\{(\beta, c) : \beta \in [r] \setminus \{\alpha\}, c \in C_\beta \setminus \{a\}, (C_\alpha \oplus (a \oplus c)) \cap C_\beta = \emptyset\}| = t - m - B_\alpha.$$

Because $a \notin C_\alpha$, adding a to C_α creates no collision within block α . Thus a tuple $y \in \mathfrak{P}(\mathcal{C})$ does not belong to $\mathfrak{P}(\mathcal{C}^{\alpha,+a})$ precisely when $y_{(\alpha)} \oplus a = y_{(\beta)} \oplus c$ for some $\beta \neq \alpha$ and $c \in C_\beta$. For any fixed $y \in \mathfrak{P}(\mathcal{C})$, the values $y_{(\beta)} \oplus c$, indexed by $\beta \in [r]$ and $c \in C_\beta$, are pairwise distinct. Hence, for fixed α , the sets $\mathcal{E}_{\alpha,\beta,c}$ are pairwise disjoint for distinct pairs (β, c) .

For $\beta \neq \alpha$ and $c \in C_\beta$, if $c = a$ or $(C_\alpha \oplus (a \oplus c)) \cap C_\beta \neq \emptyset$, Lemma 6 gives $\mathcal{E}_{\alpha,\beta,c} = \emptyset$. Consequently,

$$\mathfrak{P}(\mathcal{C}) \setminus \mathfrak{P}(\mathcal{C}^{\alpha,+a}) = \bigsqcup_{\substack{\beta \neq \alpha, c \in C_\beta \setminus \{a\}: \\ (C_\alpha \oplus (a \oplus c)) \cap C_\beta = \emptyset}} \mathcal{E}_{\alpha,\beta,c}.$$

Taking cardinalities and using Equation (25) gives

$$1 - u_\alpha = \frac{|\mathfrak{P}(\mathcal{C}) \setminus \mathfrak{P}(\mathcal{C}^{\alpha,+a})|}{|\mathfrak{P}(\mathcal{C})|} = \sum_{\substack{\beta \neq \alpha, c \in C_\beta \setminus \{a\}: \\ (C_\alpha \oplus (a \oplus c)) \cap C_\beta = \emptyset}} \frac{|\mathcal{E}_{\alpha,\beta,c}|}{|\mathfrak{P}(\mathcal{C})|}.$$

Since $(2^n - t)/(2^n - m) = 1 - (t - m)/(2^n - m)$ and the sum has $t - m - B_\alpha$ terms, the definition of d_α gives

$$d_\alpha = \frac{B_\alpha}{2^n - m} + \sum_{\substack{\beta \neq \alpha, c \in C_\beta \setminus \{a\}: \\ (C_\alpha \oplus (a \oplus c)) \cap C_\beta = \emptyset}} \left(\frac{1}{2^n - m} - \frac{|\mathcal{E}_{\alpha,\beta,c}|}{|\mathfrak{P}(\mathcal{C})|} \right).$$

Taking absolute values yields

$$|d_\alpha| \leq \frac{B_\alpha}{2^n - m} + \sum_{\substack{\beta \neq \alpha, c \in C_\beta \setminus \{a\}: \\ (C_\alpha \oplus (a \oplus c)) \cap C_\beta = \emptyset}} \left| \frac{1}{2^n - m} - \frac{|\mathcal{E}_{\alpha,\beta,c}|}{|\mathfrak{P}(\mathcal{C})|} \right|.$$

Under Equation (29), $D_t, 2^n - m \geq 3 \cdot 2^n / 4$, so the first term is at most $4B_\alpha / (3 \cdot 2^n)$. For each (β, c) in the sum, by Lemma 6,

$$\begin{aligned} \frac{1}{2^n - m} - \frac{|\mathcal{E}_{\alpha,\beta,c}|}{|\mathfrak{P}(\mathcal{C})|} &\leq \frac{1}{2^n - m} - \frac{1 - \eta_t}{2^n} \leq 2(L + 1) \frac{t}{2^{2n}}, \\ \frac{|\mathcal{E}_{\alpha,\beta,c}|}{|\mathfrak{P}(\mathcal{C})|} - \frac{1}{2^n - m} &\leq \frac{1}{D_t} - \frac{1}{2^n - m} \leq 2(L + 1) \frac{t}{2^{2n}}. \end{aligned}$$

Thus every absolute value in the sum is at most $2(L + 1)t/2^{2n}$. Since the sum has $t - m - B_\alpha$ terms,

$$|d_\alpha| \leq \frac{4B_\alpha}{3 \cdot 2^n} + 2(L + 1) \frac{t(t - m - B_\alpha)}{2^{2n}} \leq \frac{4B_\alpha}{3 \cdot 2^n} + 2(L + 1) \frac{t^2}{2^{2n}},$$

which proves Equation (33).

For $\beta \neq \alpha$, if $C_\beta = \{c\}$, a pair counted by $B_\alpha - s_\alpha$ would give an $x \in C_\alpha$ such that $x \oplus a \oplus c = c$, hence $x = a$. This contradicts $\alpha \in \mathcal{I}_a$. Hence every such pair has $s_\beta \geq 2$, and therefore

$$B_\alpha \leq s_\alpha + \sum_{\beta: s_\beta \geq 2} s_\beta.$$

Furthermore, the inequalities

$$\sum_{\alpha \in [r]} s_\alpha^2 \leq t + \Psi_t, \quad \sum_{\beta: s_\beta \geq 2} s_\beta \leq \Psi_t/2, \quad |\mathcal{I}_a| \leq t,$$

together with the inequality $(x + y)^2 \leq 2x^2 + 2y^2$, yield

$$\sum_{\alpha \in \mathcal{I}_a} B_\alpha^2 \leq 2 \sum_{\alpha \in \mathcal{I}_a} s_\alpha^2 + 2|\mathcal{I}_a| \left(\sum_{\beta: s_\beta \geq 2} s_\beta \right)^2 \leq 2(t + \Psi_t) + \frac{t}{2} \Psi_t^2.$$

This proves Equation (34). $\square$

Proposition 8. *Let $L \geq 1$ be an integer and put $\chi_t^2 := \chi^2(P_T \| Q_T)$. If $\xi_t \leq L$ and $(L + 1)t \leq 2^n/4$, then*

$$\chi_t^2 \leq 16 \frac{t + \Psi_t}{2^{3n}} + 4 \frac{t \Psi_t^2}{2^{3n}} + 16(L + 1)^2 \frac{t^5}{2^{5n}}. \quad (35)$$

Proof. For $t = 0$, both tag laws are uniform, so $\chi_0^2 = 0$. Assume henceforth $t \geq 1$. Since $|\mathcal{I}_a| = r - m$, Cauchy–Schwarz gives

$$\left(\sum_{\alpha \in \mathcal{I}_a} d_\alpha \right)^2 \leq (r - m) \sum_{\alpha \in \mathcal{I}_a} d_\alpha^2.$$

Together with Lemmas 4 and 5, this yields

$$\begin{aligned} \chi_t^2 &= \frac{2^n - m}{(2^n - t)^2} \left(\sum_{\alpha \in \mathcal{I}_a} d_\alpha^2 + \frac{(\sum_{\alpha \in \mathcal{I}_a} d_\alpha)^2}{2^n - r} \right) \\ &\leq \frac{2^n - m}{(2^n - t)^2} \left(1 + \frac{r - m}{2^n - r} \right) \sum_{\alpha \in \mathcal{I}_a} d_\alpha^2 \leq 2^{1-n} \sum_{\alpha \in \mathcal{I}_a} d_\alpha^2. \end{aligned}$$

By Equation (33),

$$d_\alpha^2 \leq 4 \frac{B_\alpha^2}{2^{2n}} + 8(L + 1)^2 \frac{t^4}{2^{4n}}.$$

Summing this inequality, using $|\mathcal{I}_a| \leq t$, and applying Equation (34) gives

$$\sum_{\alpha \in \mathcal{I}_a} d_\alpha^2 \leq 8 \frac{t + \Psi_t}{2^{2n}} + 2 \frac{t \Psi_t^2}{2^{2n}} + 8(L + 1)^2 \frac{t^5}{2^{4n}}.$$

Multiplication by 2^{1-n} proves Equation (35). $\square$

4.4 The stopped KL argument

Fix an integer $L \geq 1$ and assume $(L+1)q \leq 2^n/4$. Let $\dagger$ be a symbol outside the state spaces. In both **Real** and **Clr**, define

$$Z_t = Z_t(h, Q_t) := \begin{cases} (h, Q_t), & \xi_t \leq L, \\ \dagger, & \xi_t > L, \end{cases} \quad \text{for } 0 \leq t \leq q.$$

Let $\widetilde{\text{Real}}$ and $\widetilde{\text{Clr}}$ be the distributions of Z_q in **Real** and **Clr**, respectively. When (h, Q_t) is sampled in **Real**, write $\chi_t^2(h, Q_t)$ for the conditional divergence defined in Proposition 8. Define

$$\Gamma_L^{\text{EWC}}(q, n) := 8 \frac{q^2}{2^{3n}} + 40 \frac{q^4}{2^{4n}} + \frac{8((L+1)^2 + 4)}{3} \frac{q^6}{2^{5n}}.$$

Proposition 9. *Under $(L+1)q \leq 2^n/4$,*

$$\Delta(\widetilde{\text{Real}}, \widetilde{\text{Clr}}) \leq \sqrt{\Gamma_L^{\text{EWC}}(q, n)/2}. \quad (36)$$

Proof. Let P^{tr} and Q^{tr} be the laws of $(Z_0, \dots, Z_q)$ in **Real** and **Clr**, respectively.

For an active state $z = (h, Q_t)$ having positive probability in both worlds, the conditional next-tag laws P_T, Q_T satisfy $P_T \ll Q_T$ by the proof of Lemma 4. Given z , the adversary determines the next query, and the value of Z_{t+1} is the same deterministic function of T_{t+1} in both worlds. For brevity, we write $\mathcal{L}_W(Z_{t+1} \mid z)$ for $\mathcal{L}_W(Z_{t+1} \mid Z_t = z)$. Hence parts (i) and (ii) of Proposition 1 give

$$\begin{aligned} \mathcal{L}_{\text{Real}}(Z_{t+1} \mid z) &\ll \mathcal{L}_{\text{Clr}}(Z_{t+1} \mid z), \\ D_{\text{KL}}(\mathcal{L}_{\text{Real}}(Z_{t+1} \mid z) \parallel \mathcal{L}_{\text{Clr}}(Z_{t+1} \mid z)) &\leq \chi_t^2(h, Q_t). \end{aligned} \quad (37)$$

At $z = \dagger$, we have $\mathcal{L}_{\text{Real}}(Z_{t+1} \mid \dagger) = \mathcal{L}_{\text{Clr}}(Z_{t+1} \mid \dagger)$ and hence

$$D_{\text{KL}}(\mathcal{L}_{\text{Real}}(Z_{t+1} \mid \dagger) \parallel \mathcal{L}_{\text{Clr}}(Z_{t+1} \mid \dagger)) = 0.$$

Since an active state Z_t records the complete prefix (h, Q_t) , while $\dagger$ is absorbing, in either world $W \in \{\text{Real}, \text{Clr}\}$ we have, for every history of positive probability,

$$\mathcal{L}_W(Z_{t+1} \mid Z_0 = z_0, \dots, Z_t = z_t) = \mathcal{L}_W(Z_{t+1} \mid Z_t = z_t).$$

Hence, for any $(z_0, \dots, z_q)$,

$$P^{\text{tr}}(z_0, \dots, z_q) = \Pr_{\text{Real}}[Z_0 = z_0] \prod_{t=0}^{q-1} \Pr_{\text{Real}}[Z_{t+1} = z_{t+1} \mid Z_t = z_t],$$

and analogously for Q^{tr} . Since Z_0 has the same distribution in the two worlds, Equation (37) and the equality of the two conditional laws at $\dagger$ imply

$$P^{\text{tr}}(z_0, \dots, z_q) > 0 \implies Q^{\text{tr}}(z_0, \dots, z_q) > 0.$$

Therefore $P^{\text{tr}} \ll Q^{\text{tr}}$.

Data processing under the projection $(Z_0, \dots, Z_q) \mapsto Z_q$ and the KL chain rule, together with Equation (37) for active states and the zero divergence at $\dagger$, give

$$\begin{aligned} D_{\text{KL}}(\widetilde{\text{Real}} \parallel \widetilde{\text{Clr}}) &\leq D_{\text{KL}}(P^{\text{tr}} \parallel Q^{\text{tr}}) \\ &= \sum_{t=0}^{q-1} \mathbb{E}_{P^{\text{tr}}} [D_{\text{KL}}(\mathcal{L}_{\text{Real}}(Z_{t+1} \mid Z_t) \parallel \mathcal{L}_{\text{Clr}}(Z_{t+1} \mid Z_t))] \\ &\leq \sum_{t=0}^{q-1} \mathbb{E}_{\text{Real}} [\mathbf{1}_{\{\xi_t \leq L\}} \chi_t^2(h, Q_t)] . \end{aligned} \quad (38)$$

Since $L \geq 1$, the hypothesis implies $q \leq 2^n/8$, and hence $2^n - q \geq 2^n/2$. By Equation (18),

$$\mathbb{E}_{\text{Real}}[\Psi_t] \leq 4 \frac{t^2}{2^n}, \quad \mathbb{E}_{\text{Real}}[\Psi_t^2] \leq 16 \frac{t^2}{2^n} + 16 \frac{t^4}{2^{2n}}.$$

For every $t < q$, we also have $(L+1)t \leq 2^n/4$. Thus Proposition 8 applies on $\{\xi_t \leq L\}$ and gives

$$\begin{aligned} \mathbb{E}_{\text{Real}}[\mathbf{1}_{\{\xi_t \leq L\}} \chi_t^2(h, Q_t)] &\leq \mathbb{E}_{\text{Real}} \left[\mathbf{1}_{\{\xi_t \leq L\}} \left(16 \frac{t + \Psi_t}{2^{3n}} + 4 \frac{t \Psi_t^2}{2^{3n}} + 16(L+1)^2 \frac{t^5}{2^{5n}} \right) \right] \\ &\leq \mathbb{E}_{\text{Real}} \left[16 \frac{t + \Psi_t}{2^{3n}} + 4 \frac{t \Psi_t^2}{2^{3n}} + 16(L+1)^2 \frac{t^5}{2^{5n}} \right] \\ &\leq 16 \frac{t}{2^{3n}} + 64 \frac{t^2}{2^{4n}} + 64 \frac{t^3}{2^{4n}} + (64 + 16(L+1)^2) \frac{t^5}{2^{5n}}. \end{aligned}$$

Using this bound and the inequality

$$\sum_{t=0}^{q-1} t^k \leq \frac{q^{k+1}}{k+1} \quad k \in \{1, 2, 3, 5\}$$

in Equation (38), we obtain

$$\begin{aligned} D_{\text{KL}}(\widetilde{\text{Real}} \parallel \widetilde{\text{Clr}}) &\leq 8 \frac{q^2}{2^{3n}} + \frac{64}{3} \frac{q^3}{2^{4n}} + 16 \frac{q^4}{2^{4n}} + \frac{8((L+1)^2 + 4)}{3} \frac{q^6}{2^{5n}} \\ &\leq \Gamma_L^{\text{EWC}}(q, n). \end{aligned}$$

Part (i) of Proposition 1 gives

$$\Delta(\widetilde{\text{Real}}, \widetilde{\text{Clr}}) \leq \sqrt{\frac{1}{2} D_{\text{KL}}(\widetilde{\text{Real}} \parallel \widetilde{\text{Clr}})} \leq \sqrt{\Gamma_L^{\text{EWC}}(q, n)/2}.$$

□

Proposition 10. Under $(L+1)q \leq 2^n/4$,

$$\Delta(\mathcal{L}_{\text{Real}}(h, Q_q), \mathcal{L}_{\text{Clr}}(h, Q_q)) \leq \sqrt{\Gamma_L^{\text{EWC}}(q, n)/2} + \binom{q}{L+1} (2^n - q)^{-L}.$$

Proof. Since the map $(h, Q_q) \mapsto Z_q(h, Q_q)$ is the identity on $\{\xi_q \leq L\}$ and maps $\{\xi_q > L\}$ to $\dagger$,

$$\begin{aligned} & \Delta(\mathcal{L}_{\text{Real}}(h, Q_q), \mathcal{L}_{\text{Clr}}(h, Q_q)) - \Delta(\widetilde{\text{Real}}, \widetilde{\text{Clr}}) \\ &= \frac{1}{2} \left(\sum_{x \in \{\xi_q > L\}} |\Pr_{\text{Real}}[x] - \Pr_{\text{Clr}}[x]| - |\Pr_{\text{Real}}[\xi_q > L] - \Pr_{\text{Clr}}[\xi_q > L]| \right) \\ &\leq \min_{W \in \{\text{Real}, \text{Clr}\}} \Pr_W[\xi_q > L]. \end{aligned}$$

Hence

$$\begin{aligned} \Delta(\mathcal{L}_{\text{Real}}(h, Q_q), \mathcal{L}_{\text{Clr}}(h, Q_q)) &\leq \Delta(\widetilde{\text{Real}}, \widetilde{\text{Clr}}) + \Pr_{\text{Real}}[\xi_q > L] \\ &\leq \sqrt{\Gamma_L^{\text{EWC}}(q, n)/2} + \binom{q}{L+1} (2^n - q)^{-L}, \end{aligned}$$

where the last line follows from Equations (19) and (36). $\square$

4.5 Completing the proof of Theorem 1

Proof. Fix the adversary $\mathcal{D}$ and put $L = 5$. Since $q \leq 2^n/24$ implies $6q \leq 2^n/4$, combine the forgery reduction Equation (16), the bounds for NN_{EWC} and NC_{EWC} in Equations (17), (19) and (22), and the copy estimates in Equation (23) and Propositions 6, 7 and 10 to obtain

$$\begin{aligned} \text{Adv}_{\text{EWC}}^{\text{list-forg}}(\mathcal{D}) &\leq \frac{v}{2^n - q} + v\varepsilon + \binom{q}{2} \frac{\varepsilon}{2^n} + \frac{v}{2^n - 6q + 1} \\ &\quad + 2 \binom{q}{6} (2^n - q)^{-5} + \sqrt{\Gamma_5^{\text{EWC}}(q, n)/2}. \end{aligned}$$

By the inequality $\sqrt{x+y} \leq \sqrt{x} + \sqrt{y}$,

$$\sqrt{\Gamma_5^{\text{EWC}}(q, n)/2} \leq \frac{2q}{2^{3n/2}} + \frac{5q^2}{2^{2n}} + \frac{8q^3}{2^{5n/2}}.$$

Substitution gives the list forgery bound for $\mathcal{D}$. Maximizing over $\mathcal{D}$ and applying Proposition 2 and Lemma 2 yield Equation (15), after simplification using $1 \leq q \leq 2^n/24$. $\square$

5 Security of EWCDMD

The main result of this section is as follows.

Theorem 2. *If $1 \leq q \leq 2^n/28$, then*

$$\begin{aligned} \text{Adv}_{\text{EWCDMD}}^{\text{mac}}(q, v) \leq & \frac{(2n+8)v}{2^n} + v\varepsilon + \frac{q^2\varepsilon}{2 \cdot 2^n} + \frac{q^6}{2^{5n}} \\ & + \frac{4q}{2^{3n/2}} + \frac{6q^2}{2^{2n}} + \frac{12q^3}{2^{5n/2}} + 6\sqrt{n} \left(\frac{q}{2^n}\right)^{3/2}. \end{aligned} \quad (39)$$

By Proposition 2 and Lemma 2, it remains to bound the list forgery advantage. Fix a deterministic, adaptive, nonce-respecting adversary $\mathcal{D}$ satisfying Equation (11), and let **Real** denote the list forgery experiment of Section 3 instantiated with the EWCDMD MAC in Equation (3). For authentication query i , put

$$Y_i := P_1(N_i) \oplus h(M_i), \quad T_i := P_2(Y_i) \oplus Y_i.$$

As in the EWC analysis, $h(M_i)$ is the color and Y_i is the root of query i . Unlike EWC, equal tags need not imply equal roots because the map $y \mapsto P_2(y) \oplus y$ need not be injective.

For verification candidate j , put $Y'_j := P_1(N'_j) \oplus h(M'_j)$. Define the copy event

$$\text{Copy}_{\text{MD}} := \{\exists i \in [q], j \in [v] : N'_j = N_i, h(M'_j) = h(M_i), T'_j = T_i\}.$$

In **Real**, the conditions defining Copy_{MD} imply $Y'_j = Y_i$ and acceptance. Thus $\text{Copy}_{\text{MD}} \subseteq \text{Forge}$, and

$$\text{Forge} = \text{Copy}_{\text{MD}} \sqcup (\text{Forge} \setminus \text{Copy}_{\text{MD}}). \quad (40)$$

In Section 5.1, we bound the probability of $\text{Forge} \setminus \text{Copy}_{\text{MD}}$ in **Real**. For Copy_{MD} , we introduce the auxiliary experiments Clr_{MD} and Msg_{MD} in Section 5.2, where we bound the copy probability in Msg_{MD} and the statistical distance between the joint (h, Q_q) distributions in Msg_{MD} and Clr_{MD} . The conditional χ^2 bound in Section 5.3 and the conditional Hellinger bound in Section 5.4, together with the stopped Hellinger argument in Section 5.5, control the corresponding statistical distance between **Real** and Clr_{MD} . The estimates are assembled in Section 5.6 to obtain the MAC security bound.

5.1 Non-copy forgeries

Let π_t be the partition of $[t]$ in which indices i, j belong to the same block if and only if $Y_i = Y_j$. For any value π_t , write $\pi_t = \{I_1, \dots, I_r\}$, where $r := |\pi_t|$, with the blocks indexed by first occurrence. This partition is not part of the adversary's view. Set $\xi_0 := 0$ and $\Psi_0 := 0$. For $t \geq 1$, let

$$\xi_t := \max_{\theta \in \mathbb{F}_2^n} |\{i \leq t : T_i = \theta\}|, \quad \Psi_t := \sum_{I \in \pi_t : |I| \geq 2} |I|^2.$$

Fix $0 \leq t \leq q$ and a value (h, Q_t, π_t) having positive probability in **Real**. Write ξ_t, ψ_t for the statistics of this fixed state. For $\alpha \in [r]$, let $Y_{(\alpha)}$ be the root of I_α , so that $Y_i = Y_{(\alpha)}$ for $i \in I_\alpha$. For roots, subscripts i and (α) index queries and blocks, respectively. Let θ_α be its common tag, and put

$$C_\alpha := \{h(M_i) : i \in I_\alpha\}, \quad s_\alpha := |I_\alpha| = |C_\alpha|.$$

The last equality holds because $h(M_i) = h(M_j)$ for distinct $i, j \in I_\alpha$ would imply $P_1(N_i) = P_1(N_j)$, contradicting $N_i \neq N_j$. Unlike in **EW**C, the values θ_α need not be distinct.

Define the configuration $\mathfrak{C} := ((\theta_\alpha, C_\alpha))_{\alpha \in [r]}$ and

$$\mathfrak{P}_{\text{DM}}(\mathfrak{C}) := \left\{ (y_{(1)}, \dots, y_{(r)}) \in (\mathbb{F}_2^n)^r : \begin{array}{l} y_{(\alpha)} \neq y_{(\beta)}, \\ y_{(\alpha)} \oplus \theta_\alpha \neq y_{(\beta)} \oplus \theta_\beta, \\ (y_{(\alpha)} \oplus C_\alpha) \cap (y_{(\beta)} \oplus C_\beta) = \emptyset \\ \text{for all } \alpha \neq \beta \end{array} \right\}. \quad (41)$$

$\mathfrak{P}_{\text{DM}}(\mathfrak{C})$ is exactly the set of possible root tuples conditional on the fixed (h, Q_t, π_t) . Let $\text{Pack}_{\text{DM}}(\mathfrak{C}) := |\mathfrak{P}_{\text{DM}}(\mathfrak{C})|$.

Proposition 11. *Fix values (h, Q_t, π_t) having positive probability in **Real**. Then*

$$\Pr_{\text{Real}}[Q_t = Q_t, \pi_t = \pi_t \mid h] = \frac{\text{Pack}_{\text{DM}}(\mathfrak{C})}{(2^n)_t (2^n)_r},$$

and, conditional on (h, Q_t, π_t) , $(Y_{(1)}, \dots, Y_{(r)})$ is uniform on $\mathfrak{P}_{\text{DM}}(\mathfrak{C})$. Moreover, if $\beta \in [r]$, then after conditioning on any value of the other roots having positive conditional probability, $Y_{(\beta)}$ is uniform on a set of size at least

$$2^n - 2(r-1) - s_\beta(t - s_\beta). \quad (42)$$

For an integer $L \geq 1$, if $\xi_t \leq L$, this size is at least $2^n - (L+2)t$.

Proof. Fix a value (h, Q_t, π_t) having positive probability in **Real**. Retain the blocks I_α , their colors C_α and tags θ_α , and the configuration $\mathfrak{C}$ from Section 5.1. Write $\alpha(i) := \alpha$ for $i \in I_\alpha$. For $y = (y_{(\alpha)})_{\alpha \in [r]} \in \mathfrak{P}_{\text{DM}}(\mathfrak{C})$, define the interpolation event

$$\mathcal{E}_y^{h, Q_t, \pi_t} := \left\{ \begin{array}{ll} P_1(N_i) = y_{(\alpha(i))} \oplus h(M_i) & i \in [t], \\ P_2(y_{(\alpha)}) = y_{(\alpha)} \oplus \theta_\alpha & \alpha \in [r] \end{array} \right\}.$$

For P_1 , the inputs are distinct because the adversary is nonce-respecting, and the prescribed outputs are distinct within each block by $|C_\alpha| = s_\alpha$ and across blocks by Equation (41). The same constraints ensure distinct inputs and distinct prescribed outputs for P_2 . Since the adversary is deterministic, any pair (P_1, P_2) satisfying these constraints produces Q_t and π_t : the preceding transcript fixes each next query, and the constraints give its prescribed root and tag. Conversely, any pair producing Q_t and π_t determines a unique root tuple in $\mathfrak{P}_{\text{DM}}(\mathfrak{C})$. Hence, conditional on h ,

$$\{Q_t = Q_t, \pi_t = \pi_t\} = \bigsqcup_{y \in \mathfrak{P}_{\text{DM}}(\mathfrak{C})} \mathcal{E}_y^{h, Q_t, \pi_t}. \quad (43)$$

Independence and uniform interpolation therefore give

$$\Pr_{\text{Real}}[\mathcal{E}_y^{h, Q_t, \pi_t} \mid h] = \frac{1}{(2^n)_t (2^n)_r}.$$

Taking probabilities in Equation (43) gives

$$\begin{aligned} \Pr_{\text{Real}}[Q_t = Q_t, \pi_t = \pi_t \mid h] &= \frac{\text{Pack}_{\text{DM}}(\mathfrak{C})}{(2^n)_t (2^n)_r}, \\ \Pr_{\text{Real}}[(Y_{(\alpha)})_{\alpha \in [r]} = y \mid h, Q_t, \pi_t] &= \frac{1}{\text{Pack}_{\text{DM}}(\mathfrak{C})} \quad (y \in \mathfrak{P}_{\text{DM}}(\mathfrak{C})). \end{aligned}$$

This proves the uniform conditional root distribution.

Now fix $\alpha \in [r]$ and a value $(y_{(\beta)})_{\beta \neq \alpha}$ of the other roots having positive conditional probability. The allowed values of $Y_{(\alpha)}$ exclude $y_{(\beta)}$ and $y_{(\beta)} \oplus \theta_\beta \oplus \theta_\alpha$ for each $\beta \neq \alpha$, and $y_{(\beta)} \oplus c \oplus b$ for each $\beta \neq \alpha, c \in C_\beta, b \in C_\alpha$. Excluding these three types of values ensures distinct roots, prescribed P_2 outputs, and prescribed P_1 outputs, respectively. The uniform distribution on $\mathfrak{P}_{\text{DM}}(\mathfrak{C})$ makes $Y_{(\alpha)}$ uniform on the remaining values, whose number is at least

$$2^n - 2(r-1) - |C_\alpha| \sum_{\beta \neq \alpha} |C_\beta| = 2^n - 2(r-1) - s_\alpha(t - s_\alpha).$$

This proves Equation (42). If $\xi_t \leq L$, then $s_\alpha(t - s_\alpha) \leq Lt$. Together with $r \leq t$, this gives the final bound. $\square$

For an integer $L \geq 1$, we next bound the probability of $\text{Forge} \setminus \text{Copy}_{\text{MD}}$ on $\{\xi_q \leq L\}$, and then bound $\Pr_{\text{Real}}[\xi_q > L]$.

Proposition 12. *Let $1 \leq L < 2^n$, $q \geq 1$, and assume $(L+2)q < 2^n$. Then*

$$\Pr_{\text{Real}}[(\text{Forge} \setminus \text{Copy}_{\text{MD}}) \cap \{\xi_q \leq L\}] \leq \frac{v}{2^n - q} + \frac{Lv}{2^n - (L+2)q}. \quad (44)$$

Proof. Fix a value (h, Q_q, π_q) having positive probability in Real and satisfying $\xi_q \leq L$. It determines the verification list. Put $r := |\pi_q|$ and, for candidate $j \in [v]$, define the events

$$\begin{aligned} \text{Forge}_j &:= \{T'_j = P_2(Y'_j) \oplus Y'_j\}, \\ \text{Copy}_{\text{MD},j} &:= \{\exists i \in [q] : N'_j = N_i, h(M'_j) = h(M_i), T'_j = T_i\}, \\ \mathcal{F}_j^{\text{new}} &:= \text{Forge}_j \cap \{Y'_j \notin \{Y_{(\alpha)} : \alpha \in [r]\}\}, \\ \mathcal{F}_j^{\text{old}} &:= \text{Forge}_j \cap \{Y'_j \in \{Y_{(\alpha)} : \alpha \in [r]\}\}. \end{aligned}$$

In Real , taking the unions of Forge_j and $\text{Copy}_{\text{MD},j}$ over $j \in [v]$ gives Forge and Copy_{MD} , respectively. Moreover, $\text{Copy}_{\text{MD},j} \subseteq \mathcal{F}_j^{\text{old}}$, so

$$\text{Forge}_j \setminus \text{Copy}_{\text{MD},j} = \mathcal{F}_j^{\text{new}} \sqcup (\mathcal{F}_j^{\text{old}} \setminus \text{Copy}_{\text{MD},j}).$$

A union bound therefore gives

$$\begin{aligned} & \Pr_{\text{Real}}[\text{Forge} \setminus \text{Copy}_{\text{MD}} \mid h, Q_q, \pi_q] \\ & \leq \sum_{j=1}^v \Pr_{\text{Real}}[\mathcal{F}_j^{\text{new}} \mid h, Q_q, \pi_q] + \sum_{j=1}^v \Pr_{\text{Real}}[\mathcal{F}_j^{\text{old}} \setminus \text{Copy}_{\text{MD},j} \mid h, Q_q, \pi_q]. \end{aligned}$$

Fix $j \in [v]$. For $\mathcal{F}_j^{\text{new}}$, condition further on a value (y, y') of $((Y_{(\alpha)})_{\alpha \in [r]}, Y'_j)$ having positive conditional probability in **Real** given (h, Q_q, π_q) , with $y = (y_{(\alpha)})_{\alpha \in [r]}$ and $y' \notin \{y_{(\alpha)} : \alpha \in [r]\}$. Conditioning on (h, Q_q, π_q, y, y') fixes the q previously queried pairs of P_1 and the r previously queried pairs of P_2 ; the remaining P_2 outputs are still uniform among the unused values. Acceptance requires $P_2(y') = y' \oplus T'_j$, which has probability either zero or $(2^n - r)^{-1}$. Averaging over y and y' gives

$$\Pr_{\text{Real}}[\mathcal{F}_j^{\text{new}} \mid h, Q_q, \pi_q] \leq \frac{1}{2^n - r} \leq \frac{1}{2^n - q}. \quad (45)$$

We next bound $\mathcal{F}_j^{\text{old}} \setminus \text{Copy}_{\text{MD},j}$. Only blocks in

$$\mathcal{B}_j := \{\alpha \in [r] : \theta_\alpha = T'_j\}$$

can contribute. Since $\xi_q \leq L$, we have $|\mathcal{B}_j| \leq L$. Suppose first that N'_j is a new nonce. The event $\text{Copy}_{\text{MD},j}$ is then impossible. Condition further on $(Y_{(\alpha)})_{\alpha \in [r]} = y$ having positive conditional probability in **Real** given (h, Q_q, π_q) . Under this conditioning, $P_1(N'_j)$ is uniform on the $2^n - q$ unused outputs. Each equality $Y'_j = Y_{(\alpha)}$ with $\alpha \in \mathcal{B}_j$ specifies at most one of these outputs. A union bound and averaging over the root tuple give

$$\Pr_{\text{Real}}[\mathcal{F}_j^{\text{old}} \setminus \text{Copy}_{\text{MD},j} \mid h, Q_q, \pi_q] \leq \frac{|\mathcal{B}_j|}{2^n - q} \leq \frac{L}{2^n - q}.$$

Now suppose $N'_j = N_i$ for the unique index $i \in I_{\alpha_0}$. If $h(M'_j) = h(M_i)$, then $\mathcal{F}_j^{\text{old}} \setminus \text{Copy}_{\text{MD},j}$ is impossible. If $h(M'_j) \neq h(M_i)$,

$$Y'_j = Y_{(\alpha_0)} \oplus h(M_i) \oplus h(M'_j) \neq Y_{(\alpha_0)}.$$

For $\alpha \in \mathcal{B}_j \setminus \{\alpha_0\}$, condition further on $(Y_{(\beta)})_{\beta \neq \alpha} = y_{-\alpha}$ having positive conditional probability in **Real** given (h, Q_q, π_q) . The value of Y'_j is then fixed. By Proposition 11, $Y_{(\alpha)}$ is uniform on at least $2^n - (L + 2)q$ possible values, and hence

$$\Pr_{\text{Real}}[Y'_j = Y_{(\alpha)} \mid h, Q_q, \pi_q, (Y_{(\beta)})_{\beta \neq \alpha} = y_{-\alpha}] \leq \frac{1}{2^n - (L + 2)q}.$$

Averaging over $(Y_{(\beta)})_{\beta \neq \alpha}$ and taking a union bound over $\mathcal{B}_j \setminus \{\alpha_0\}$ give

$$\Pr_{\text{Real}}[\mathcal{F}_j^{\text{old}} \setminus \text{Copy}_{\text{MD},j} \mid h, Q_q, \pi_q] \leq \frac{L}{2^n - (L + 2)q}.$$

Combining the two nonce cases with Equation (45) and the union bound above gives

$$\Pr_{\text{Real}}[\text{Forge} \setminus \text{Copy}_{\text{MD}} \mid h, Q_q, \pi_q] \leq \frac{v}{2^n - q} + \frac{Lv}{2^n - (L+2)q}.$$

Multiplying by $\mathbf{1}_{\{\xi_q \leq L\}}$ and averaging over (h, Q_q, π_q) proves Equation (44). $\square$

We next bound the probability that $\xi_q > L$. Let $\mathfrak{B}_m$ denote the m th Bell number, the number of partitions of $[m]$, with $\mathfrak{B}_6 = 203$.

Lemma 8. *Assume $q \leq 2^n$. For every integer $L \geq 1$,*

$$\Pr_{\text{Real}}[\xi_q > L] \leq \tau_L^{\text{MD}} := \binom{q}{L+1} \frac{2^n \mathfrak{B}_{L+1}}{(2^n - q + 1)^{L+1}}. \quad (46)$$

Here $\binom{q}{L+1} = 0$ when $L \geq q$.

Proof. If $L \geq q$, then $\xi_q \leq q \leq L$, so the bound is immediate. Hence assume $L < q$ and put $m := L + 1$. For $\theta \in \mathbb{F}_2^n$, define

$$\kappa_\theta := |\{y \in \mathbb{F}_2^n : P_2(y) \oplus y = \theta\}|.$$

Hence we have

$$\kappa_\theta^m = \sum_{(y_1, \dots, y_m) \in (\mathbb{F}_2^n)^m} \mathbf{1}\{P_2(y_j) = y_j \oplus \theta \text{ for all } j \in [m]\}.$$

Taking expectations gives

$$\begin{aligned} \mathbb{E}_{P_2}[\kappa_\theta^m] &= \sum_{(y_1, \dots, y_m) \in (\mathbb{F}_2^n)^m} \Pr_{P_2}[P_2(y_j) = y_j \oplus \theta \text{ for all } j \in [m]] \\ &= \sum_{\pi \in \mathcal{P}_m} \sum_{\substack{z_1, \dots, z_{|\pi|} \in \mathbb{F}_2^n \\ z_1, \dots, z_{|\pi|} \text{ distinct}}} \Pr_{P_2}[P_2(z_\ell) = z_\ell \oplus \theta \text{ for all } \ell \in [|\pi|]] \\ &= \sum_{\pi \in \mathcal{P}_m} (2^n)^{|\pi|} \frac{1}{(2^n)^{|\pi|}} \\ &= \sum_{\pi \in \mathcal{P}_m} 1 = \mathfrak{B}_m, \end{aligned}$$

where $\mathcal{P}_m$ is the set of partitions of $[m]$.

Fix $\theta \in \mathbb{F}_2^n$. For each $i \in [q]$, condition on a positive-probability value of $H_{i-1} := (h, P_2, Q_{i-1}, Y_1, \dots, Y_{i-1})$ in Real. Then the next query and the $i-1$ previously assigned outputs of P_1 are determined. The fresh output $P_1(N_i)$ is uniform over the other $2^n - i + 1$ values, and at most κ_θ of them yield tag θ . Hence

$$\Pr_{\text{Real}}[T_i = \theta \mid H_{i-1}] \leq \frac{\kappa_\theta}{2^n - i + 1} \leq \frac{\kappa_\theta}{2^n - q + 1}.$$

Fix positions $1 \leq i_1 < \dots < i_m \leq q$ and define the event

$$E_r := \{T_{i_1} = \dots = T_{i_r} = \theta\}, \quad r \in [m],$$

with E_0 the sure event. Since E_{r-1} is determined by $H_{i_{r-1}}$,

$$\begin{aligned} \Pr_{\text{Real}}[E_r \mid H_{i_{r-1}}] &= \Pr_{\text{Real}}[E_{r-1} \mid H_{i_{r-1}}] \Pr_{\text{Real}}[T_{i_r} = \theta \mid H_{i_{r-1}}] \\ &\leq \Pr_{\text{Real}}[E_{r-1} \mid H_{i_{r-1}}] \frac{\kappa_\theta}{2^n - q + 1}. \end{aligned}$$

Averaging over $(h, Q_{i_{r-1}}, Y_1, \dots, Y_{i_{r-1}})$ gives

$$\Pr_{\text{Real}}[E_r \mid P_2] \leq \frac{\kappa_\theta}{2^n - q + 1} \Pr_{\text{Real}}[E_{r-1} \mid P_2].$$

Iterating over $r = 1, \dots, m$ yields

$$\Pr_{\text{Real}}[T_{i_1} = \dots = T_{i_m} = \theta \mid P_2] \leq \left(\frac{\kappa_\theta}{2^n - q + 1} \right)^m.$$

Averaging over P_2 and using $\mathbb{E}_{P_2}[\kappa_\theta^m] = \mathfrak{B}_m$, we obtain

$$\Pr_{\text{Real}}[T_{i_1} = \dots = T_{i_m} = \theta] \leq \frac{\mathfrak{B}_m}{(2^n - q + 1)^m}.$$

Hence, by a union bound,

$$\begin{aligned} \Pr_{\text{Real}}[\xi_q > L] &\leq \sum_{\theta \in \mathbb{F}_2^n} \sum_{1 \leq i_1 < \dots < i_m \leq q} \Pr_{\text{Real}}[T_{i_1} = \dots = T_{i_m} = \theta] \\ &\leq \sum_{\theta \in \mathbb{F}_2^n} \sum_{1 \leq i_1 < \dots < i_m \leq q} \frac{\mathfrak{B}_m}{(2^n - q + 1)^m} \\ &= \binom{q}{m} \frac{2^n \mathfrak{B}_m}{(2^n - q + 1)^m} = \tau_L^{\text{MD}}. \end{aligned}$$

This proves Equation (46). $\square$

Under the assumptions of Proposition 12, split $\text{Forge} \setminus \text{Copy}_{\text{MD}}$ according to whether $\xi_q \leq L$. Then Equation (40) and Equations (44) and (46) give

$$\begin{aligned} &\Pr_{\text{Real}}[\text{Forge}] \\ &\leq \Pr_{\text{Real}}[\text{Copy}_{\text{MD}}] + \Pr_{\text{Real}}[(\text{Forge} \setminus \text{Copy}_{\text{MD}}) \cap \{\xi_q \leq L\}] + \Pr_{\text{Real}}[\xi_q > L] \\ &\leq \Pr_{\text{Real}}[\text{Copy}_{\text{MD}}] + \frac{v}{2^n - q} + \frac{Lv}{2^n - (L+2)q} + \tau_L^{\text{MD}}. \end{aligned} \tag{47}$$

5.2 The copy event and auxiliary experiments

It remains to bound $\Pr_{\text{Real}}[\text{Copy}_{\text{MD}}]$. Since $\mathcal{D}$ is deterministic, Q_q determines its verification list, so this event is determined by (h, Q_q) . We introduce two auxiliary authentication experiments, Clr_{MD} and Msg_{MD} , identical to Real except for the authentication oracle. In both experiments, h and P_2 are sampled independently as in Real . For each key realization, an authentication query (N, M) generates a latent root Y and returns the tag T as follows:

$$\begin{aligned} \text{Clr}_{\text{MD}} : \quad Y &:= \Pi_{h(M)}(N), \quad T := P_2(Y) \oplus Y, \\ \text{Msg}_{\text{MD}} : \quad Y &:= \Pi_M(N), \quad T := P_2(Y) \oplus Y. \end{aligned}$$

When an index is encountered for the first time, the corresponding $\Pi_{h(M)}$ or Π_M is sampled as an independent uniform permutation; later queries with the same index reuse it. All these permutations are mutually independent and independent of (h, P_2) .

In Msg_{MD} , transcript generation does not use h , so AXU bounds the copy event after the transcript is fixed. We therefore compare Msg_{MD} with Clr_{MD} , and then compare Real with Clr_{MD} . Applying the event bound for statistical distance twice gives

$$\begin{aligned} \Pr_{\text{Real}}[\text{Copy}_{\text{MD}}] &\leq \Pr_{\text{Msg}_{\text{MD}}}[\text{Copy}_{\text{MD}}] + \Delta(\mathcal{L}_{\text{Msg}_{\text{MD}}}(h, Q_q), \mathcal{L}_{\text{Clr}_{\text{MD}}}(h, Q_q)) \\ &\quad + \Delta(\mathcal{L}_{\text{Real}}(h, Q_q), \mathcal{L}_{\text{Clr}_{\text{MD}}}(h, Q_q)). \end{aligned} \tag{48}$$

Proposition 13.

$$\Pr_{\text{Msg}_{\text{MD}}}[\text{Copy}_{\text{MD}}] \leq v\varepsilon.$$

The proof is identical to that of Proposition 6.

Proposition 14. *Assume $q < 2^n$. Then*

$$\Delta(\mathcal{L}_{\text{Msg}_{\text{MD}}}(h, Q_q), \mathcal{L}_{\text{Clr}_{\text{MD}}}(h, Q_q)) \leq \binom{q}{2} \frac{\varepsilon}{2^n}.$$

Proof. For the adversary $\mathcal{D}$ fixed in Section 5, condition on $P_2 = p$. We construct an EWC adversary $\mathcal{D}'_p$ as follows. It runs $\mathcal{D}$, forwards each authentication query submitted by $\mathcal{D}$ to the Clr or Msg oracle, and returns $p(Y) \oplus Y$ upon receiving the response Y . It then outputs $\mathcal{D}$'s verification list. Thus $\mathcal{D}'_p$ is deterministic and preserves the query counts, nonce-respecting property, and pair freshness required in Section 4.

For a query–response transcript $R_q := ((N_i, M_i, Y_i))_{i=1}^q$ of $\mathcal{D}'_p$, define the map Φ_p by

$$\Phi_p(h, R_q) := (h, ((N_i, M_i, p(Y_i) \oplus Y_i))_{i=1}^q).$$

With superscripts specifying the EWC adversary, the above simulation gives

$$\begin{aligned} \mathcal{L}_{\text{Clr}_{\text{MD}}}(h, Q_q \mid P_2 = p) &= (\Phi_p)_\# \mathcal{L}_{\text{Clr}}^{\mathcal{D}'_p}(h, R_q), \\ \mathcal{L}_{\text{Msg}_{\text{MD}}}(h, Q_q \mid P_2 = p) &= (\Phi_p)_\# \mathcal{L}_{\text{Msg}}^{\mathcal{D}'_p}(h, R_q). \end{aligned}$$

Since P_2 is uniformly distributed in both experiments, averaging over its value and applying Equation (6) give

$$\begin{aligned} & \Delta(\mathcal{L}_{\text{Msg}_{\text{MD}}}(h, Q_q), \mathcal{L}_{\text{Clr}_{\text{MD}}}(h, Q_q)) \\ & \leq \frac{1}{(2^n)!} \sum_{p \in \text{Perm}(\mathbb{F}_2^n)} \Delta(\mathcal{L}_{\text{Msg}}^{\mathcal{D}'_p}(h, R_q), \mathcal{L}_{\text{Clr}}^{\mathcal{D}'_p}(h, R_q)) \leq \binom{q}{2} \frac{\varepsilon}{2^n}, \end{aligned}$$

where the last inequality follows from Proposition 7. $\square$

It remains to compare the joint (h, Q_q) distributions in **Real** and **Clr_{MD}**. We first record moment bounds for Ψ_t .

Lemma 9. *Assume $q < 2^n$. For $W \in \{\text{Real}, \text{Clr}_{\text{MD}}\}$ and $0 \leq t \leq q$,*

$$\mathbb{E}_W[\Psi_t] \leq \frac{2t^2}{2^n - q}, \quad \mathbb{E}_W[\Psi_t^2] \leq \frac{8t^2}{2^n - q} + \frac{4t^4}{(2^n - q)^2}.$$

Proof. Fix $W \in \{\text{Real}, \text{Clr}_{\text{MD}}\}$, $i \in [q]$, and $y \in \mathbb{F}_2^n$, and condition on a positive-probability value of $H_{i-1} := (h, P_2, Q_{i-1}, Y_1, \dots, Y_{i-1})$ in W . In **Real**, the fresh P_1 output is uniform on $2^n - i + 1$ values; in **Clr_{MD}**, the fresh output of the relevant color permutation is uniform on at least $2^n - i + 1$ values. Since $Y_i = y$ specifies at most one such output, in either case

$$\Pr_W[Y_i = y \mid H_{i-1}] \leq \frac{1}{2^n - q}.$$

Apply Lemma 1 with $Z_i = Y_i$ and $D = 2^n - q$. $\square$

5.3 Conditional divergence between the join distributions

Fix $0 \leq t \leq q$. In **Real**, distinct nonces of the same color have distinct roots, so the corresponding color permutations in **Clr_{MD}** can interpolate all nonce-root pairs. With the same values of h and P_2 , this reproduces the transcript and root partition with positive probability. Hence

$$\mathcal{L}_{\text{Real}}(h, Q_t, \pi_t) \ll \mathcal{L}_{\text{Clr}_{\text{MD}}}(h, Q_t, \pi_t).$$

In this subsection we fix $0 \leq t < q$ and a value $\omega_t := (h, Q_t, \pi_t)$ having positive probability in **Real**. All conditional laws below are given this state. We retain the notation $Y_{(\alpha)}, \theta_\alpha, C_\alpha, s_\alpha$ and the configuration $\mathfrak{C}$ from Equation (41). The adversary determines the next query from Q_t . Write

$$a := h(M_{t+1}), \quad m := |\{i \in [t] : h(M_i) = a\}|, \quad \mathcal{I}_a := \{\alpha \in [r] : a \notin C_\alpha\}.$$

For $\alpha \in \mathcal{I}_a$, write $\mathfrak{C}^{\alpha, +a}$ for the configuration obtained by adding a to C_α , and set

$$u_\alpha := \frac{\text{Pack}_{\text{DM}}(\mathfrak{C}^{\alpha, +a})}{\text{Pack}_{\text{DM}}(\mathfrak{C})}, \quad d_\alpha := u_\alpha - \frac{2^n - t}{2^n - m}. \quad (49)$$

Encode the next root by a variable $J \in \mathcal{I}_a \cup \{\star\}$: set $J := \alpha$ if $Y_{t+1} = Y_{(\alpha)}$, and set $J := \star$ if Y_{t+1} is a new root. The eligible old blocks are precisely the $r - m$ elements of $\mathcal{I}_a$. Let $P_J^{\omega_t}$ and $Q_J^{\omega_t}$ be the conditional laws of J in Real and Clr_{MD} , respectively.

Lemma 10. *For $\alpha \in \mathcal{I}_a$,*

$$\begin{aligned} P_J^{\omega_t}(\alpha) &= \frac{u_\alpha}{2^n - t}, & P_J^{\omega_t}(\star) &= 1 - \sum_{\alpha \in \mathcal{I}_a} P_J^{\omega_t}(\alpha), \\ Q_J^{\omega_t}(\alpha) &= \frac{1}{2^n - m}, & Q_J^{\omega_t}(\star) &= \frac{2^n - r}{2^n - m}. \end{aligned}$$

Proof. Fix $\alpha \in \mathcal{I}_a$. In Real , condition further on $(Y_{(\beta)})_{\beta \in [r]} = y$, where y has positive conditional probability given ω_t . The fresh output $P_1(N_{t+1})$ is uniform over the $2^n - t$ unused values. The next root equals $y_{(\alpha)}$ precisely when this output is $y_{(\alpha)} \oplus a$, which is unused if and only if $y \in \mathfrak{P}_{\text{DM}}(\mathfrak{C}^{\alpha, +a})$. Averaging over the uniform conditional root distribution by Proposition 11 gives

$$P_J^{\omega_t}(\alpha) = \Pr_{\text{Real}}[J = \alpha \mid \omega_t] = \frac{1}{2^n - t} \frac{\text{Pack}_{\text{DM}}(\mathfrak{C}^{\alpha, +a})}{\text{Pack}_{\text{DM}}(\mathfrak{C})} = \frac{u_\alpha}{2^n - t}.$$

The formula for $P_J^{\omega_t}(\star)$ follows by taking the complement of the old-root branches.

In Clr_{MD} , condition further on $(Y_{(\beta)})_{\beta \in [r]} = y$, where y has positive conditional probability given ω_t . The color- a permutation has already produced m distinct roots, and its next output is uniform over the other $2^n - m$ values. The available old roots are the $r - m$ roots indexed by $\mathcal{I}_a$; the remaining $2^n - r$ values give a new root. Averaging over the root tuple therefore gives

$$\begin{aligned} Q_J^{\omega_t}(\alpha) &= \Pr_{\text{Clr}_{\text{MD}}}[J = \alpha \mid \omega_t] = \frac{1}{2^n - m} \quad (\alpha \in \mathcal{I}_a), \\ Q_J^{\omega_t}(\star) &= \Pr_{\text{Clr}_{\text{MD}}}[J = \star \mid \omega_t] = \frac{2^n - r}{2^n - m}. \end{aligned}$$

□

Next we fix $L \geq 1$ and assume

$$\xi_t \leq L, \quad (L + 2)t \leq 2^n/4. \quad (50)$$

Put

$$D_t := 2^n - (L + 2)t, \quad \eta_t := \frac{(L + 2)t}{D_t}.$$

Thus $D_t \geq 3 \cdot 2^n/4$ and $\eta_t \leq 1/3$. For $\alpha \in \mathcal{I}_a$, $\beta \in [r]$, and $c \in C_\beta \setminus \{a\}$, define

$$\mathcal{E}_{\alpha, \beta, c} := \{y \in \mathfrak{P}_{\text{DM}}(\mathfrak{C}) : y_{(\alpha)} \oplus a = y_{(\beta)} \oplus c\}.$$

For $\alpha \in \mathcal{I}_a$, call a pair (β, c) with $\beta \in [r]$ and $c \in C_\beta \setminus \{a\}$ compatible with α if

$$\beta \neq \alpha, \quad ((a \oplus c) \oplus C_\alpha) \cap C_\beta = \emptyset, \quad a \oplus c \neq \theta_\alpha \oplus \theta_\beta. \quad (51)$$

Lemma 11. *If (β, c) is incompatible with α , then $\mathcal{E}_{\alpha, \beta, c} = \emptyset$. Otherwise,*

$$\frac{1 - \eta_t}{2^n} \leq \frac{|\mathcal{E}_{\alpha, \beta, c}|}{|\mathfrak{P}_{\text{DM}}(\mathfrak{C})|} \leq \frac{1}{D_t}.$$

Proof. If $\beta = \alpha$, the defining equality forces $a = c$, contrary to the choice of c . Suppose $\beta \neq \alpha$. If $((a \oplus c) \oplus C_\alpha) \cap C_\beta \neq \emptyset$, choose $x \in C_\alpha$ and $w := x \oplus a \oplus c \in C_\beta$. Every $y \in \mathcal{E}_{\alpha, \beta, c}$ would satisfy

$$y_{(\alpha)} \oplus x = y_{(\beta)} \oplus a \oplus c \oplus x = y_{(\beta)} \oplus w,$$

contradicting the distinct prescribed P_1 outputs. If $a \oplus c = \theta_\alpha \oplus \theta_\beta$, every such tuple would satisfy

$$y_{(\alpha)} \oplus \theta_\alpha = y_{(\beta)} \oplus a \oplus c \oplus \theta_\alpha = y_{(\beta)} \oplus \theta_\beta,$$

contradicting the distinct prescribed P_2 outputs. Thus $\mathcal{E}_{\alpha, \beta, c} = \emptyset$ whenever (β, c) is incompatible with α .

Assume henceforth that (β, c) is compatible with α . Let $\mathfrak{C}_{-\alpha}$ be the configuration obtained by deleting block α . Since $\mathfrak{P}_{\text{DM}}(\mathfrak{C})$ is nonempty, so is $\mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha})$. For $z = (z_{(\gamma)})_{\gamma \neq \alpha} \in \mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha})$, write z^{+u} for the full tuple whose α th coordinate is u and whose remaining coordinates are those of z , and put

$$\begin{aligned} \mathcal{S}(z) &:= \{u \in \mathbb{F}_2^n : z^{+u} \in \mathfrak{P}_{\text{DM}}(\mathfrak{C})\}, \\ \mathcal{G} &:= \{z \in \mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha}) : z_{(\beta)} \oplus a \oplus c \in \mathcal{S}(z)\}. \end{aligned}$$

Deleting the α th coordinate gives

$$\begin{aligned} |\mathfrak{P}_{\text{DM}}(\mathfrak{C})| &= \sum_{z \in \mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha})} |\mathcal{S}(z)|, \\ |\mathcal{E}_{\alpha, \beta, c}| &= |\mathcal{G}| \leq |\mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha})|. \end{aligned} \tag{52}$$

For fixed $z \in \mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha})$, a value u is excluded from $\mathcal{S}(z)$ only if, for some $\gamma \neq \alpha$, either $u = z_{(\gamma)}$, $u \oplus \theta_\alpha = z_{(\gamma)} \oplus \theta_\gamma$, or $u \oplus x = z_{(\gamma)} \oplus w$ for some $x \in C_\alpha$ and $w \in C_\gamma$. These are respectively collisions between roots, prescribed P_2 outputs, and prescribed P_1 outputs. Since $r \leq t$ and $s_\gamma \leq \xi_t \leq L$ for every block γ , we have

$$|\mathcal{S}(z)| \geq 2^n - 2(r-1) - s_\alpha(t - s_\alpha) \geq D_t.$$

It follows from Equation (52) that

$$\frac{|\mathcal{E}_{\alpha, \beta, c}|}{|\mathfrak{P}_{\text{DM}}(\mathfrak{C})|} \leq \frac{|\mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha})|}{D_t |\mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha})|} = \frac{1}{D_t}.$$

We next give the counting estimate used for the lower bound. For $\gamma \notin \{\alpha, \beta\}$ and $\zeta \in \mathbb{F}_2^n$, define

$$\mathcal{A}_{\beta, \gamma, \zeta} := \{z \in \mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha}) : z_{(\beta)} = z_{(\gamma)} \oplus \zeta\}.$$

Deleting coordinate β maps $\mathcal{A}_{\beta,\gamma,\zeta}$ injectively into $\mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha,-\beta})$, where $\mathfrak{C}_{-\alpha,-\beta}$ is obtained by deleting blocks α and β . The same count of forbidden values shows that each tuple in the latter set has at least

$$2^n - 2(r-2) - s_\beta(t - s_\alpha - s_\beta) \geq D_t$$

extensions in $\mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha})$. Therefore,

$$|\mathcal{A}_{\beta,\gamma,\zeta}| \leq |\mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha,-\beta})| \leq \frac{|\mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha})|}{D_t}. \quad (53)$$

Compatibility prevents all three types of collision between blocks α and β . Hence a tuple $z \in \mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha}) \setminus \mathcal{G}$ must satisfy, for some $\gamma \notin \{\alpha, \beta\}$, at least one of

$$\begin{aligned} z_{(\beta)} \oplus a \oplus c &= z_{(\gamma)}, \\ z_{(\beta)} \oplus a \oplus c \oplus \theta_\alpha &= z_{(\gamma)} \oplus \theta_\gamma, \\ z_{(\beta)} \oplus a \oplus c \oplus x &= z_{(\gamma)} \oplus w \quad (x \in C_\alpha, w \in C_\gamma). \end{aligned}$$

Each equality defines a set of the form $\mathcal{A}_{\beta,\gamma,\zeta}$, whose cardinality is bounded by Equation (53). Their number is at most

$$2(r-2) + s_\alpha \sum_{\gamma \notin \{\alpha, \beta\}} s_\gamma = 2(r-2) + s_\alpha(t - s_\alpha - s_\beta) \leq (L+2)t.$$

Thus

$$\begin{aligned} |\mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha}) \setminus \mathcal{G}| &\leq \frac{(L+2)t}{D_t} |\mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha})| = \eta_t |\mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha})|, \\ |\mathcal{G}| &\geq (1 - \eta_t) |\mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha})|. \end{aligned}$$

Finally, $|\mathcal{S}(z)| \leq 2^n$ for every tuple $z \in \mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha})$, so Equation (52) gives

$$\frac{|\mathcal{E}_{\alpha,\beta,c}|}{|\mathfrak{P}_{\text{DM}}(\mathfrak{C})|} \geq \frac{(1 - \eta_t) |\mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha})|}{2^n |\mathfrak{P}_{\text{DM}}(\mathfrak{C}_{-\alpha})|} = \frac{1 - \eta_t}{2^n}.$$

□

For $\alpha \in \mathcal{I}_a$, define

$$B_\alpha^{\text{MD}} := |\{(\beta, c) : \beta \in [r], c \in C_\beta \setminus \{a\}, (\beta, c) \text{ is not compatible}\}|. \quad (54)$$

Lemma 12. *Let $L \geq 1$. If $\xi_t \leq L$ and $(L+2)t \leq 2^n/4$, then, for every $\alpha \in \mathcal{I}_a$,*

$$|d_\alpha| \leq \frac{4B_\alpha^{\text{MD}}}{3 \cdot 2^n} + 2(L+2) \frac{t^2}{2^{2n}}, \quad (55)$$

and

$$\sum_{\alpha \in \mathcal{I}_a} (B_\alpha^{\text{MD}})^2 \leq 3(t + \Psi_t) + \frac{3t}{4} \Psi_t^2 + 3Lt^2. \quad (56)$$

Proof. Fix $\alpha \in \mathcal{I}_a$. Since exactly m blocks contain a and $\sum_{\beta=1}^r s_\beta = t$, the number of pairs (β, c) with $\beta \in [r]$ and $c \in C_\beta \setminus \{a\}$ is $t - m$. By Equation (54), B_α^{MD} of these pairs are incompatible with α , so

$$|\{(\beta, c) : (\beta, c) \text{ is compatible with } \alpha\}| = t - m - B_\alpha^{\text{MD}}.$$

Because $a \notin C_\alpha$, adding a to C_α creates no collision within block α . It leaves the root and P_2 constraints unchanged. Thus a tuple $y \in \mathfrak{P}_{\text{DM}}(\mathfrak{C})$ does not belong to $\mathfrak{P}_{\text{DM}}(\mathfrak{C}^{\alpha, +a})$ precisely when $y_{(\alpha)} \oplus a = y_{(\beta)} \oplus c$ for some $\beta \neq \alpha$ and $c \in C_\beta$. The case $c = a$ would force equal roots and is impossible. For any fixed tuple $y \in \mathfrak{P}_{\text{DM}}(\mathfrak{C})$, the prescribed P_1 outputs $y_{(\beta)} \oplus c$, indexed by $\beta \in [r]$ and $c \in C_\beta$, are pairwise distinct. Therefore the sets $\mathcal{E}_{\alpha, \beta, c}$ are pairwise disjoint for distinct pairs (β, c) . By Lemma 11, incompatible pairs give $\mathcal{E}_{\alpha, \beta, c} = \emptyset$, and hence

$$\mathfrak{P}_{\text{DM}}(\mathfrak{C}) \setminus \mathfrak{P}_{\text{DM}}(\mathfrak{C}^{\alpha, +a}) = \bigsqcup_{\substack{(\beta, c) \text{ compatible} \\ \text{with } \alpha}} \mathcal{E}_{\alpha, \beta, c}. \quad (57)$$

Taking cardinalities in Equation (57) and using Equation (49) give

$$1 - u_\alpha = \frac{|\mathfrak{P}_{\text{DM}}(\mathfrak{C}) \setminus \mathfrak{P}_{\text{DM}}(\mathfrak{C}^{\alpha, +a})|}{|\mathfrak{P}_{\text{DM}}(\mathfrak{C})|} = \sum_{\substack{(\beta, c) \text{ compatible} \\ \text{with } \alpha}} \frac{|\mathcal{E}_{\alpha, \beta, c}|}{|\mathfrak{P}_{\text{DM}}(\mathfrak{C})|}.$$

Since $(2^n - t)/(2^n - m) = 1 - (t - m)/(2^n - m)$ and the sum has $t - m - B_\alpha^{\text{MD}}$ terms, the definition of d_α gives

$$d_\alpha = \frac{B_\alpha^{\text{MD}}}{2^n - m} + \sum_{\substack{(\beta, c) \text{ compatible} \\ \text{with } \alpha}} \left(\frac{1}{2^n - m} - \frac{|\mathcal{E}_{\alpha, \beta, c}|}{|\mathfrak{P}_{\text{DM}}(\mathfrak{C})|} \right). \quad (58)$$

Taking absolute values in Equation (58) yields

$$|d_\alpha| \leq \frac{B_\alpha^{\text{MD}}}{2^n - m} + \sum_{\substack{(\beta, c) \text{ compatible} \\ \text{with } \alpha}} \left| \frac{1}{2^n - m} - \frac{|\mathcal{E}_{\alpha, \beta, c}|}{|\mathfrak{P}_{\text{DM}}(\mathfrak{C})|} \right|.$$

Under Equation (50), $D_t, 2^n - m \geq 3 \cdot 2^n / 4$, so the first term is at most $4B_\alpha^{\text{MD}} / (3 \cdot 2^n)$. For each compatible pair, Lemma 11 gives

$$\begin{aligned} \frac{1}{2^n - m} - \frac{|\mathcal{E}_{\alpha, \beta, c}|}{|\mathfrak{P}_{\text{DM}}(\mathfrak{C})|} &\leq \frac{1}{2^n - m} - \frac{1 - \eta_t}{2^n} \leq 2(L + 2) \frac{t}{2^{2n}}, \\ \frac{|\mathcal{E}_{\alpha, \beta, c}|}{|\mathfrak{P}_{\text{DM}}(\mathfrak{C})|} - \frac{1}{2^n - m} &\leq \frac{1}{D_t} - \frac{1}{2^n - m} \leq 2(L + 2) \frac{t}{2^{2n}}. \end{aligned}$$

Thus every absolute value in the sum is at most $2(L + 2)t/2^{2n}$. Using the number of compatible pairs, we obtain

$$|d_\alpha| \leq \frac{4B_\alpha^{\text{MD}}}{3 \cdot 2^n} + 2(L + 2) \frac{t(t - m - B_\alpha^{\text{MD}})}{2^{2n}} \leq \frac{4B_\alpha^{\text{MD}}}{3 \cdot 2^n} + 2(L + 2) \frac{t^2}{2^{2n}},$$

which proves Equation (55).

For the second estimate, put

$$A_t := \sum_{\beta: s_\beta \geq 2} s_\beta, \quad b_z := |\{(\beta, c) : \beta \in [r], c \in C_\beta, c \oplus \theta_\beta = z\}| \quad (z \in \mathbb{F}_2^n).$$

The s_α pairs from block α are incompatible. For $\beta \neq \alpha$, if $C_\beta = \{c\}$ and the translation condition in Equation (51) fails, there is an $x \in C_\alpha$ such that $x \oplus a \oplus c = c$, hence $x = a$. This contradicts $\alpha \in \mathcal{I}_a$. Thus every external pair violating this condition belongs to a block of size at least two, and there are at most A_t such pairs. The remaining incompatibility, a collision of prescribed P_2 outputs, requires $c \oplus \theta_\beta = a \oplus \theta_\alpha$ and contributes at most $b_{a \oplus \theta_\alpha}$ pairs. Consequently,

$$B_\alpha^{\text{MD}} \leq s_\alpha + A_t + b_{a \oplus \theta_\alpha}. \quad (59)$$

Furthermore,

$$\sum_{\alpha \in [r]} s_\alpha^2 \leq t + \Psi_t, \quad A_t \leq \Psi_t/2, \quad \sum_{z \in \mathbb{F}_2^n} b_z = t, \quad |\mathcal{I}_a| \leq t.$$

Since $\xi_t \leq L$, each tag occurs in at most L root blocks. Grouping blocks by their tags therefore gives

$$\sum_{\alpha \in [r]} b_{a \oplus \theta_\alpha}^2 \leq L \sum_{z \in \mathbb{F}_2^n} b_z^2 \leq L \left(\sum_{z \in \mathbb{F}_2^n} b_z \right)^2 = Lt^2.$$

Summing Equation (59) over $\alpha \in \mathcal{I}_a$, applying $(x + y + z)^2 \leq 3(x^2 + y^2 + z^2)$ and using the preceding estimates yields Equation (56). $\square$

Proposition 15. *Let $L \geq 1$. If $\xi_t \leq L$ and $(L + 2)t \leq 2^n/4$, then*

$$\chi^2(P_J^{\omega_t} \| Q_J^{\omega_t}) \leq \frac{64}{3} \frac{t + \Psi_t + Lt^2}{2^{3n}} + \frac{16}{3} \frac{t\Psi_t^2}{2^{3n}} + 16(L + 2)^2 \frac{t^5}{2^{5n}}. \quad (60)$$

Proof. Retain the notation of Section 5.3. Substituting Equation (49) and Lemma 10 into the definition of χ^2 and applying Cauchy-Schwarz with $|\mathcal{I}_a| = r - m$ give

$$\begin{aligned} \chi^2(P_J^{\omega_t} \| Q_J^{\omega_t}) &= \frac{2^n - m}{(2^n - t)^2} \left(\sum_{\alpha \in \mathcal{I}_a} d_\alpha^2 + \frac{(\sum_{\alpha \in \mathcal{I}_a} d_\alpha)^2}{2^n - r} \right) \\ &\leq \frac{2^n - m}{(2^n - t)^2} \left(1 + \frac{r - m}{2^n - r} \right) \sum_{\alpha \in \mathcal{I}_a} d_\alpha^2 \\ &\leq \frac{2^{2n}}{(2^n - t)^3} \sum_{\alpha \in \mathcal{I}_a} d_\alpha^2 \leq 2^{1-n} \sum_{\alpha \in \mathcal{I}_a} d_\alpha^2. \end{aligned}$$

By Equation (55),

$$d_\alpha^2 \leq \frac{32(B_\alpha^{\text{MD}})^2}{9 \cdot 2^{2n}} + 8(L+2)^2 \frac{t^4}{2^{4n}}.$$

Summing this inequality, using $|\mathcal{I}_a| \leq t$, and applying Equation (56) gives

$$\sum_{\alpha \in \mathcal{I}_a} d_\alpha^2 \leq \frac{32}{3} \frac{t + \Psi_t + Lt^2}{2^{2n}} + \frac{8}{3} \frac{t\Psi_t^2}{2^{2n}} + 8(L+2)^2 \frac{t^5}{2^{4n}}.$$

Multiplication by 2^{1-n} proves Equation (60). $\square$

5.4 Conditional distance between the new-root tag distributions

Fix $0 \leq t < q$ with $q \leq 2^n/4$ and a value $\omega_t = (h, Q_t, \pi_t)$ as in Section 5.3. We retain the notation $a, r, m, \mathcal{I}_a$, and J from that subsection. For every $\alpha \in \mathcal{I}_a$, since $\mathfrak{P}_{\text{DM}}(\mathfrak{C}^{\alpha, +a}) \subseteq \mathfrak{P}_{\text{DM}}(\mathfrak{C})$, we have $u_\alpha \leq 1$. Consequently, the new-root branch has positive probability in both experiments:

$$Q_J^{\omega_t}(\star) = \frac{2^n - r}{2^n - m} > 0, \quad P_J^{\omega_t}(\star) \geq 1 - \frac{r - m}{2^n - t} > 0. \quad (61)$$

First fix a root tuple $Y_{(1)}, \dots, Y_{(r)}$ such that $(\omega_t, Y_{(1)}, \dots, Y_{(r)}, J = \star)$ has positive probability in **Real**, and set

$$\mathcal{A} := \{Y_{(1)}, \dots, Y_{(r)}\}, \quad \mathcal{B} := \{Y_{(\alpha)} \oplus \theta_\alpha : \alpha \in [r]\},$$

and

$$S_a := \{Y_i \oplus h(M_i) \oplus a : i \leq t\}, \quad G := S_a \setminus \mathcal{A}.$$

Conditional on $(\omega_t, Y_{(1)}, \dots, Y_{(r)})$, the fresh P_1 output makes Y_{t+1} uniform on $\mathbb{F}_2^n \setminus S_a$. Conditioning further on $J = \star$, Y_{t+1} is uniform on $(\mathbb{F}_2^n \setminus \mathcal{A}) \setminus G$. For $z \in \mathbb{F}_2^n$, define

$$\mathfrak{p}(z) := \Pr_{\text{Real}}[T_{t+1} = z \mid \omega_t, Y_{(1)}, \dots, Y_{(r)}, J = \star].$$

Likewise, fix a root tuple $Y_{(1)}, \dots, Y_{(r)}$ such that $(\omega_t, Y_{(1)}, \dots, Y_{(r)}, J = \star)$ has positive probability in **ClrMD**, with $\mathcal{A}$ and $\mathcal{B}$ as above. Given $(\omega_t, Y_{(1)}, \dots, Y_{(r)}, J = \star)$, Y_{t+1} is uniform on $\mathbb{F}_2^n \setminus \mathcal{A}$. For $z \in \mathbb{F}_2^n$, define

$$\mathfrak{q}(z) := \Pr_{\text{ClrMD}}[T_{t+1} = z \mid \omega_t, Y_{(1)}, \dots, Y_{(r)}, J = \star].$$

Fourier technique. We use Fourier analysis on the additive group $(\mathbb{F}_2^n, \oplus)$; see O'Donnell [23] for background. Related recent applications of Fourier analysis to permutation-based constructions can be found in [14,15]. For $\zeta, x \in \mathbb{F}_2^n$, let $\chi_\zeta(x) := (-1)^{\zeta \cdot x}$, where the inner product is over $\mathbb{F}_2$ and $\chi_0 = 1$ is the trivial character. For real functions φ, ψ on $\mathbb{F}_2^n$, define the unnormalized Fourier transform and XOR convolution by

$$\widehat{\varphi}(\zeta) := \sum_x \varphi(x) \chi_\zeta(x), \quad (\varphi * \psi)(z) := \sum_x \varphi(x) \psi(z \oplus x).$$

Fourier expansion, the convolution identity, and Parseval's identity give

$$\begin{aligned}\varphi(x) &= \frac{1}{2^n} \sum_{\zeta} \widehat{\varphi}(\zeta) \chi_{\zeta}(x), & \widehat{\varphi * \psi}(\zeta) &= \widehat{\varphi}(\zeta) \widehat{\psi}(\zeta), \\ \|\varphi\|_2^2 &= \sum_x |\varphi(x)|^2 = \frac{1}{2^n} \sum_{\zeta} |\widehat{\varphi}(\zeta)|^2.\end{aligned}$$

Set

$$\Lambda(\mathcal{B}) := \max_{\zeta \neq 0} |\widehat{\mathbf{1}_{\mathcal{B}}}(\zeta)|^2.$$

Proposition 16. *Let u be uniform on $\mathbb{F}_2^n$. Then*

$$\chi^2(\mathbf{p} \| u) \leq 8\Lambda(\mathcal{B}) \frac{t}{2^{3n}}, \quad \chi^2(\mathbf{q} \| u) \leq 3\Lambda(\mathcal{B}) \frac{r}{2^{3n}}. \quad (62)$$

Proof. Fix $W \in \{\text{Real}, \text{Clr}_{\text{MD}}\}$ and a state $\omega_t = (h, Q_t, \pi_t)$ as in Section 5.4. Condition on $(\omega_t, Y_{(1)}, \dots, Y_{(r)}, J = \star)$ having positive probability in W . Retain the notation of that subsection. The state ω_t and root tuple $Y_{(1)}, \dots, Y_{(r)}$ impose separate interpolation constraints on P_2 and on P_1 or the color permutations. The additional event $J = \star$ concerns only the freshness of the next root. Thus the remaining P_2 is a uniform bijection from $\mathcal{A}^c$ to $\mathcal{B}^c$. To treat both experiments together, put

$$(F, \mathbf{v}) := \begin{cases} (\mathcal{A} \cup G, \mathbf{p}), & \text{in Real,} \\ (\mathcal{A}, \mathbf{q}), & \text{in Clr}_{\text{MD}}, \end{cases} \quad d := |F|.$$

In each case, Y_{t+1} is uniform on F^c , and $(Y_{t+1}, P_2(Y_{t+1}))$ is uniform on $F^c \times \mathcal{B}^c$. For any $z \in \mathbb{F}_2^n$, the system

$$\begin{cases} P_2(Y_{t+1}) \oplus Y_{t+1} = z, \\ (Y_{t+1}, P_2(Y_{t+1})) \in F^c \times \mathcal{B}^c \end{cases}$$

has

$$|F^c \cap (\mathcal{B}^c \oplus z)| = 2^n - d - r + |F \cap (\mathcal{B} \oplus z)| = 2^n - d - r + (\mathbf{1}_F * \mathbf{1}_{\mathcal{B}})(z)$$

solutions for the pair $(Y_{t+1}, P_2(Y_{t+1}))$. Since u is uniform on $\mathbb{F}_2^n$, we have

$$\chi^2(\mathbf{v} \| u) = 2^n \sum_{z \in \mathbb{F}_2^n} \left(\mathbf{v}(z) - \frac{1}{2^n} \right)^2.$$

By the definition of $\mathbf{v}$ and the preceding count, for every $z \in \mathbb{F}_2^n$,

$$\mathbf{v}(z) - \frac{1}{2^n} = \frac{|F^c \cap (\mathcal{B}^c \oplus z)|}{|F^c| |\mathcal{B}^c|} - \frac{1}{2^n} = \frac{(\mathbf{1}_F * \mathbf{1}_{\mathcal{B}})(z) - dr/2^n}{(2^n - d)(2^n - r)}. \quad (63)$$

The constant term in the Fourier expansion of $\mathbf{1}_F * \mathbf{1}_B$ is $dr/2^n$. By Parseval's identity and the convolution identity,

$$\begin{aligned} \sum_{z \in \mathbb{F}_2^n} ((\mathbf{1}_F * \mathbf{1}_B)(z) - dr/2^n)^2 &= \frac{1}{2^n} \sum_{\zeta \neq 0} |\widehat{\mathbf{1}_F}(\zeta)|^2 |\widehat{\mathbf{1}_B}(\zeta)|^2 \\ &\leq \frac{\Lambda(B)}{2^n} \sum_{\zeta \neq 0} |\widehat{\mathbf{1}_F}(\zeta)|^2 \\ &= \Lambda(B) \left(d - \frac{d^2}{2^n} \right). \end{aligned}$$

Substituting Equation (63) into the preceding expression for $\chi^2(\mathbf{v}||u)$ and applying this estimate gives

$$\chi^2(\mathbf{v}||u) \leq \frac{\Lambda(B)d}{(2^n - d)(2^n - r)^2}.$$

In Real, $d = r + |G| \leq 2t$; in Clr_{MD}, $d = r \leq t$. Since $t \leq 2^n/4$, we obtain

$$\begin{aligned} \chi^2(\mathbf{p}||u) &\leq \frac{64}{9} \Lambda(B) \frac{t}{2^{3n}} \leq 8 \Lambda(B) \frac{t}{2^{3n}}, \\ \chi^2(\mathbf{q}||u) &\leq \frac{64}{27} \Lambda(B) \frac{r}{2^{3n}} \leq 3 \Lambda(B) \frac{r}{2^{3n}}. \end{aligned}$$

□

Lemma 13. For $W \in \{\text{Real}, \text{Clr}_{\text{MD}}\}$ and $1 \leq t \leq q$,

$$\mathbb{E}_W[\Lambda^2(B)] \leq 8t^2(\log(2^{n+1}t) + 1)^2. \quad (64)$$

Proof. Fix $W \in \{\text{Real}, \text{Clr}_{\text{MD}}\}$ and $1 \leq t \leq q$. Here B denotes the random set of P_2 outputs assigned during these t queries, and the expectation is taken over the full experiment W . We may sample the outputs of P_2 as follows. Independently of h and P_1 in Real, or of h and the color permutations in Clr_{MD}, sample a uniform ordering $V_1, \dots, V_{2^n}$ of $\mathbb{F}_2^n$. Whenever a new root is first queried, assign the next unused V_j as its P_2 output; repeated roots reuse their assigned outputs. At each new root, this selects a uniform unused output, so it gives the same distribution as a uniform permutation P_2 , also for adaptive queries.

Let r be the number of distinct roots among the first t queries. Then $B = \{V_1, \dots, V_r\}$. For fixed $k \in [t]$ and $\zeta \in \mathbb{F}_2^n \setminus \{0\}$, put $S_{k,\zeta} := \sum_{j=1}^k \chi_\zeta(V_j)$. The first k entries of the sampled ordering form a uniform sample without replacement, and the nontrivial character χ_ζ takes each of the values $+1$ and -1 exactly 2^{n-1} times. Hoeffding's comparison for sampling without replacement [19] therefore gives, for every $\lambda \in \mathbb{R}$,

$$\mathbb{E}_W[e^{\lambda S_{k,\zeta}}] \leq \left(\frac{e^\lambda + e^{-\lambda}}{2} \right)^k = (\cosh \lambda)^k \leq e^{k\lambda^2/2}.$$

The value of r may depend on the outputs already assigned. We bound each joint event involving $r = k$ by the corresponding unconditional tail probability.

Applying Chernoff's bound to $S_{k,\zeta}$ and $-S_{k,\zeta}$ with parameter z/k gives, for every $z > 0$,

$$\Pr_W[r = k, |S_{k,\zeta}| \geq z] \leq \Pr[|S_{k,\zeta}| \geq z] \leq 2e^{-z^2/(2k)} \leq 2e^{-z^2/(2t)}.$$

By the definition of Λ and the identity $\mathcal{B} = \{V_1, \dots, V_r\}$,

$$\Lambda^{1/2}(\mathcal{B}) = \max_{\zeta \neq 0} \left| \sum_{j=1}^r \chi_\zeta(V_j) \right|.$$

A union bound over $k \in [t]$ and the $2^n - 1$ nontrivial characters, using $2t(2^n - 1) \leq 2^{n+1}t$, therefore yields

$$\Pr_W[\Lambda^{1/2}(\mathcal{B}) \geq z] \leq \min\{1, 2^{n+1}t e^{-z^2/(2t)}\}.$$

Applying the tail-integral formula to the fourth moment of $\Lambda^{1/2}(\mathcal{B})$ and splitting the integral at $z = \sqrt{2t \log(2^{n+1}t)}$, where the two tail bounds coincide, gives

$$\begin{aligned} \mathbb{E}_W[\Lambda^2(\mathcal{B})] &= 4 \int_0^\infty z^3 \Pr_W[\Lambda^{1/2}(\mathcal{B}) \geq z] \, dz \\ &\leq 4 \int_0^{\sqrt{2t \log(2^{n+1}t)}} z^3 \, dz + 4 \cdot 2^{n+1}t \int_{\sqrt{2t \log(2^{n+1}t)}}^\infty z^3 e^{-z^2/(2t)} \, dz \\ &= 4t^2 \log^2(2^{n+1}t) + 8t^2 (\log(2^{n+1}t) + 1) \\ &\leq 8t^2 (\log(2^{n+1}t) + 1)^2. \end{aligned}$$

This proves Equation (64). $\square$

Now we condition on $(\omega_t, J = \star)$ having positive probability in **Real**. Let $\mathbf{p}'_{\omega_t}$ and $\mathbf{q}'_{\omega_t}$ denote the resulting laws of T_{t+1} in **Real** and **Clr_{MD}**, respectively. Thus $\mathbf{p}'_{\omega_t}$ is obtained by averaging $\mathbf{p}$ over the conditional root distribution in **Real**, and $\mathbf{q}'_{\omega_t}$ by averaging $\mathbf{q}$ in **Clr_{MD}**. Put

$$A_P(\omega_t) := \mathbb{E}_{\text{Real}}[\Lambda(\mathcal{B}) \mid \omega_t, J = \star], \quad A_Q(\omega_t) := \mathbb{E}_{\text{Clr}_{\text{MD}}}[\Lambda(\mathcal{B}) \mid \omega_t, J = \star].$$

Proposition 17. *If $q \leq 2^n/4$, then*

$$H^2(\mathbf{p}'_{\omega_t}, \mathbf{q}'_{\omega_t}) \leq 16 \frac{t}{2^{3n}} A_P(\omega_t) + 6 \frac{t}{2^{3n}} A_Q(\omega_t). \quad (65)$$

Proof. Let u be uniform on $\mathbb{F}_2^n$. By convexity of $\chi^2(\cdot \| u)$,

$$\begin{aligned} \chi^2(\mathbf{p}'_{\omega_t} \| u) &\leq \mathbb{E}_{\text{Real}}[\chi^2(\mathbf{p} \| u) \mid \omega_t, J = \star], \\ \chi^2(\mathbf{q}'_{\omega_t} \| u) &\leq \mathbb{E}_{\text{Clr}_{\text{MD}}}[\chi^2(\mathbf{q} \| u) \mid \omega_t, J = \star]. \end{aligned}$$

Applying Proposition 16 inside these expectations gives

$$\chi^2(\mathbf{p}'_{\omega_t} \| u) \leq 8 \frac{t}{2^{3n}} A_P(\omega_t), \quad \chi^2(\mathbf{q}'_{\omega_t} \| u) \leq 3 \frac{t}{2^{3n}} A_Q(\omega_t).$$

Then the triangle inequality for H , followed by $(x+y)^2 \leq 2x^2 + 2y^2$ and $H^2 \leq \chi^2$, proves the claim. $\square$

Given ω_t , the next query is fixed, and Q_{t+1} is obtained by appending this query and T_{t+1} to Q_t . The value of J determines π_{t+1} : add $t+1$ to I_α if $J = \alpha$, or add the singleton block $\{t+1\}$ if $J = \star$.

Lemma 14. *For a value ω_t fixed above, let $P_{J,T_{t+1}}^{\omega_t}$ and $Q_{J,T_{t+1}}^{\omega_t}$ be the conditional laws of (J, T_{t+1}) given ω_t in Real and Clr_{MD}, respectively. Then*

$$H^2(P_{J,T_{t+1}}^{\omega_t}, Q_{J,T_{t+1}}^{\omega_t}) = H^2(P_J^{\omega_t}, Q_J^{\omega_t}) + \sqrt{P_J^{\omega_t}(\star) Q_J^{\omega_t}(\star)} H^2(\mathbf{p}'_{\omega_t}, \mathbf{q}'_{\omega_t}).$$

Proof. On an old-root branch $J = \alpha$, both experiments return the fixed tag θ_α , so the corresponding conditional Hellinger term is zero. On $J = \star$, the two conditional tag laws are precisely $\mathbf{p}'_{\omega_t}$ and $\mathbf{q}'_{\omega_t}$. Thus Equation (8) gives the identity. $\square$

Conditional on ω_t , the next extended state ω_{t+1} is obtained from (J, T_{t+1}) in both Real and Clr_{MD}. Data processing therefore gives

$$H^2(\mathcal{L}_{\text{Real}}(\omega_{t+1} \mid \omega_t), \mathcal{L}_{\text{Clr}_{\text{MD}}}(\omega_{t+1} \mid \omega_t)) \leq H^2(P_{J,T_{t+1}}^{\omega_t}, Q_{J,T_{t+1}}^{\omega_t}).$$

5.5 The stopped Hellinger argument

Fix an integer $L \geq 1$ and assume $(L+2)q \leq 2^n/4$. Let $\dagger$ be a symbol outside the extended-state spaces. In both Real and Clr_{MD}, define

$$Z_t := Z_t(h, Q_t, \pi_t) := \begin{cases} (h, Q_t, \pi_t), & \xi_t \leq L, \\ \dagger, & \xi_t > L, \end{cases} \quad \text{for } 0 \leq t \leq q.$$

Let $\widetilde{\text{Real}}$ and $\widetilde{\text{Clr}_{\text{MD}}}$ be the distributions of Z_q in Real and Clr_{MD}, respectively. Define

$$\begin{aligned} \Gamma_L^{\text{MD}}(q, n) &:= \frac{32}{3} \frac{q^2}{2^{3n}} + \frac{64L}{9} \frac{q^3}{2^{3n}} + \frac{128}{9} \frac{q^3}{(2^n - q)2^{3n}} + \frac{32}{3} \frac{q^4}{(2^n - q)2^{3n}} \\ &\quad + \frac{32}{9} \frac{q^6}{(2^n - q)^2 \cdot 2^{3n}} + \frac{8(L+2)^2}{3} \frac{q^6}{2^{5n}} \\ &\quad + \frac{44\sqrt{2}}{3} (\log(2^{n+1}q) + 1) \frac{q^3}{2^{3n}}. \end{aligned}$$

Proposition 18. *If $q \geq 1$ and $(L+2)q \leq 2^n/4$, then*

$$\Delta(\widetilde{\text{Real}}, \widetilde{\text{Clr}_{\text{MD}}}) \leq \sqrt{\Gamma_L^{\text{MD}}(q, n)}.$$

Proof. Use the stopped process Z_t from Section 5.5. Define

$$\mathcal{S}_t^{\text{act}} := \{z_t \neq \dagger : \Pr_{\text{Real}}[Z_t = z_t] \Pr_{\text{Clr}_{\text{MD}}}[Z_t = z_t] > 0\}.$$

For $z_t \in \mathcal{S}_t^{\text{act}}$, use the conditional laws from Sections 5.3 and 5.4 with state argument z_t . Define

$$\begin{aligned} \mathbf{J}_t &:= \sum_{z_t \in \mathcal{S}_t^{\text{act}}} \sqrt{\Pr_{\text{Real}}[Z_t = z_t] \Pr_{\text{ClrMD}}[Z_t = z_t]} H^2(P_J^{z_t}, Q_J^{z_t}), \\ \mathbf{N}_t &:= \sum_{z_t \in \mathcal{S}_t^{\text{act}}} \sqrt{\Pr_{\text{Real}}[Z_t = z_t] \Pr_{\text{ClrMD}}[Z_t = z_t]} P_J^{z_t}(\star) Q_J^{z_t}(\star) H^2(\mathbf{p}'_{z_t}, \mathbf{q}'_{z_t}). \end{aligned}$$

Write $Z_{0:t} := (Z_0, \dots, Z_t)$ and let $z_{0:t} := (z_0, \dots, z_t)$ denote a value of this history. Applying Equation (7) to the laws of $Z_{0:q}$ in Real and ClrMD gives

$$\begin{aligned} &H^2(\mathcal{L}_{\text{Real}}(Z_{0:q}), \mathcal{L}_{\text{ClrMD}}(Z_{0:q})) \\ &= H^2(\mathcal{L}_{\text{Real}}(Z_0), \mathcal{L}_{\text{ClrMD}}(Z_0)) + \sum_{t=0}^{q-1} \sum_{z_{0:t}} \sqrt{\Pr_{\text{Real}}[Z_{0:t} = z_{0:t}] \Pr_{\text{ClrMD}}[Z_{0:t} = z_{0:t}]} \\ &\quad \cdot H^2(\mathcal{L}_{\text{Real}}(Z_{t+1} \mid Z_{0:t} = z_{0:t}), \mathcal{L}_{\text{ClrMD}}(Z_{t+1} \mid Z_{0:t} = z_{0:t})). \end{aligned}$$

The initial term is zero because the laws of Z_0 coincide. For each $t \in \{0, \dots, q-1\}$, if $z_t = \dagger$, the last Hellinger distance is zero since $Z_{t+1} = \dagger$ with probability 1 in both experiments. If $z_t \neq \dagger$, the event $\{Z_{0:t} = z_{0:t}\}$ equals $\{Z_t = z_t\}$ in both experiments. Hence we have

$$\begin{aligned} H^2(\mathcal{L}_{\text{Real}}(Z_{0:q}), \mathcal{L}_{\text{ClrMD}}(Z_{0:q})) &= \sum_{t=0}^{q-1} \sum_{z_t \in \mathcal{S}_t^{\text{act}}} \sqrt{\Pr_{\text{Real}}[Z_t = z_t] \Pr_{\text{ClrMD}}[Z_t = z_t]} \\ &\quad \cdot H^2(\mathcal{L}_{\text{Real}}(Z_{t+1} \mid Z_t = z_t), \mathcal{L}_{\text{ClrMD}}(Z_{t+1} \mid Z_t = z_t)). \end{aligned}$$

At each such state $z_t \in \mathcal{S}_t^{\text{act}}$, (J, T_{t+1}) determines Z_{t+1} in both experiments. Data processing and Lemma 14 then give

$$\begin{aligned} &H^2(\mathcal{L}_{\text{Real}}(Z_{t+1} \mid Z_t = z_t), \mathcal{L}_{\text{ClrMD}}(Z_{t+1} \mid Z_t = z_t)) \\ &\leq H^2(P_J^{z_t}, Q_J^{z_t}) + \sqrt{P_J^{z_t}(\star) Q_J^{z_t}(\star)} H^2(\mathbf{p}'_{z_t}, \mathbf{q}'_{z_t}). \end{aligned}$$

Summing these two terms with the preceding weights gives $\mathbf{J}_t + \mathbf{N}_t$. Finally, data processing under $Z_{0:q} \mapsto Z_q$, whose laws are Real and ClrMD , yields

$$H^2(\widetilde{\text{Real}}, \widetilde{\text{ClrMD}}) \leq \sum_{t=0}^{q-1} (\mathbf{J}_t + \mathbf{N}_t). \quad (66)$$

Moment estimates. Fix $0 \leq t < q$. We now bound $\mathbf{J}_t$ and $\mathbf{N}_t$. For $W \in \{\text{Real}, \text{ClrMD}\}$ and $z_t \in \mathcal{S}_t^{\text{act}}$,

$$\Pr_W[Z_t = z_t] = \Pr_W[(h, Q_t, \pi_t) = z_t],$$

because z_t satisfies $\xi_t \leq L$. Write $\Psi_t(z_t)$ for its root statistic. For $k \in \{1, 2\}$, Cauchy–Schwarz gives

$$\begin{aligned} & \sum_{z_t \in \mathcal{S}_t^{\text{act}}} \sqrt{\Pr_{\text{Real}}[Z_t = z_t] \Pr_{\text{ClrMD}}[Z_t = z_t]} \Psi_t^k(z_t) \\ & \leq \prod_{W \in \{\text{Real}, \text{ClrMD}\}} \left(\mathbb{E}_W[\Psi_t^k \mathbf{1}_{\{\xi_t \leq L\}}] \right)^{1/2}. \end{aligned}$$

Here each expectation includes all active states in its experiment. Dropping the indicators and applying Lemma 9 yield

$$\sum_{z_t \in \mathcal{S}_t^{\text{act}}} \sqrt{\Pr_{\text{Real}}[Z_t = z_t] \Pr_{\text{ClrMD}}[Z_t = z_t]} \Psi_t(z_t) \leq \frac{2t^2}{2^n - q}, \quad (67)$$

$$\sum_{z_t \in \mathcal{S}_t^{\text{act}}} \sqrt{\Pr_{\text{Real}}[Z_t = z_t] \Pr_{\text{ClrMD}}[Z_t = z_t]} \Psi_t^2(z_t) \leq \frac{8t^2}{2^n - q} + \frac{4t^4}{(2^n - q)^2}. \quad (68)$$

The join contribution. By $H^2 \leq \chi^2$ and Proposition 15, for every common active state,

$$H^2(P_J^{z_t}, Q_J^{z_t}) \leq \frac{64}{3} \frac{t + \Psi_t(z_t) + Lt^2}{2^{3n}} + \frac{16}{3} \frac{t\Psi_t^2(z_t)}{2^{3n}} + 16(L+2)^2 \frac{t^5}{2^{5n}}.$$

The sum of the state weights $\sqrt{\Pr_{\text{Real}}[Z_t = z_t] \Pr_{\text{ClrMD}}[Z_t = z_t]}$ is at most one. Substituting the pointwise bound in the definition of J_t and using Equations (67) and (68) therefore give

$$J_t \leq \frac{64}{3} \frac{t + Lt^2}{2^{3n}} + \frac{128}{3} \frac{t^2 + t^3}{(2^n - q)2^{3n}} + \frac{64}{3} \frac{t^5}{(2^n - q)^2 \cdot 2^{3n}} + 16(L+2)^2 \frac{t^5}{2^{5n}}.$$

The new-root contribution. Use $A_P(z_t)$ and $A_Q(z_t)$ from Section 5.4. Here $\mathcal{B}$ is the set of P_2 outputs assigned during the first t queries in the corresponding experiment, and J is the branch of query $t+1$. For each $z_t \in \mathcal{S}_t^{\text{act}}$, the event $\{Z_t = z_t, J = \star\}$ has positive probability in both experiments by Equation (61), so these conditional expectations are defined. By Proposition 17,

$$N_t \leq 16 \frac{t}{2^{3n}} S_{P,t} + 6 \frac{t}{2^{3n}} S_{Q,t},$$

where

$$\begin{aligned} S_{P,t} &:= \sum_{z_t \in \mathcal{S}_t^{\text{act}}} \sqrt{\Pr_{\text{Real}}[Z_t = z_t] P_J^{z_t}(\star) \Pr_{\text{ClrMD}}[Z_t = z_t] Q_J^{z_t}(\star)} A_P(z_t), \\ S_{Q,t} &:= \sum_{z_t \in \mathcal{S}_t^{\text{act}}} \sqrt{\Pr_{\text{Real}}[Z_t = z_t] P_J^{z_t}(\star) \Pr_{\text{ClrMD}}[Z_t = z_t] Q_J^{z_t}(\star)} A_Q(z_t). \end{aligned}$$

For an active state,

$$\Pr_{\text{Real}}[Z_t = z_t]P_J^{z_t}(\star) = \Pr_{\text{Real}}[Z_t = z_t, J = \star],$$

and the analogous identity holds in Clr_{MD} . Cauchy–Schwarz, followed by conditional Jensen, gives

$$\begin{aligned} S_{P,t}^2 &\leq \left(\sum_{z_t \in S_t^{\text{act}}} \Pr_{\text{Real}}[Z_t = z_t, J = \star] A_P^2(z_t) \right) \left(\sum_{z_t \in S_t^{\text{act}}} \Pr_{\text{Clr}_{\text{MD}}}[Z_t = z_t, J = \star] \right) \\ &\leq \sum_{z_t \in S_t^{\text{act}}} \Pr_{\text{Real}}[Z_t = z_t, J = \star] \mathbb{E}_{\text{Real}}[\Lambda^2(\mathcal{B}) \mid Z_t = z_t, J = \star] \\ &\leq \mathbb{E}_{\text{Real}}[\Lambda^2(\mathcal{B}) \mathbf{1}_{\{\xi_t \leq L, J = \star\}}] \leq \mathbb{E}_{\text{Real}}[\Lambda^2(\mathcal{B})]. \end{aligned}$$

The penultimate inequality extends the sum to all active states in Real and uses total expectation. Interchanging the experiments gives $S_{Q,t}^2 \leq \mathbb{E}_{\text{Clr}_{\text{MD}}}[\Lambda^2(\mathcal{B})]$. For $t \geq 1$, Lemma 13 consequently gives

$$S_{P,t}, S_{Q,t} \leq \sqrt{8} t (\log(2^{n+1}q) + 1).$$

For $t = 0$, $\mathcal{B} = \emptyset$ and both sums vanish. Hence, in all cases,

$$\mathbf{N}_t \leq 44\sqrt{2} (\log(2^{n+1}q) + 1) \frac{t^2}{2^{3n}}.$$

Summing the contributions. Substituting these estimates into Equation (66), using $\sum_{t < q} t^k \leq q^{k+1}/(k+1)$ for $k \in \{1, 2, 3, 5\}$, and applying $\Delta \leq H$ proves the claim. $\square$

Proposition 19. *Let $1 \leq L < 2^n$ be an integer and let $q \geq 1$. If $(L+2)q \leq 2^n/4$, then*

$$\Delta(\mathcal{L}_{\text{Real}}(h, Q_q), \mathcal{L}_{\text{Clr}_{\text{MD}}}(h, Q_q)) \leq \sqrt{\Gamma_L^{\text{MD}}(q, n)} + \tau_L^{\text{MD}}.$$

Proof. The map $(h, Q_q, \pi_q) \mapsto Z_q(h, Q_q, \pi_q)$ fixes each state with $\xi_q \leq L$ and sends every other state to $\dagger$. As in the proof of Proposition 10, merging these latter states gives

$$\begin{aligned} &\Delta(\mathcal{L}_{\text{Real}}(h, Q_q, \pi_q), \mathcal{L}_{\text{Clr}_{\text{MD}}}(h, Q_q, \pi_q)) \\ &\leq \Delta(\widetilde{\text{Real}}, \widetilde{\text{Clr}_{\text{MD}}}) + \min_{W \in \{\text{Real}, \text{Clr}_{\text{MD}}\}} \Pr_W[\xi_q > L]. \end{aligned}$$

Projecting onto (h, Q_q) and applying Proposition 18 and Lemma 8 prove the claim. $\square$

5.6 Completing the proof of Theorem 2

Proof (of Theorem 2). Fix the adversary $\mathcal{D}$ and put $L = 5$. Since $q \leq 2^n/28$ implies $7q \leq 2^n/4$, combine Equations (47) and (48) and Propositions 13, 14 and 19 to obtain

$$\text{Adv}_{\text{EWCDMD}}^{\text{list-forg}}(\mathcal{D}) \leq v\varepsilon + \binom{q}{2} \frac{\varepsilon}{2^n} + \frac{v}{2^n - q} + \frac{5v}{2^n - 7q} + 2\tau_5^{\text{MD}} + \sqrt{\Gamma_5^{\text{MD}}(q, n)}.$$

Since $\mathfrak{B}_6 = 203$ and $2^n - q + 1 \geq 27 \cdot 2^n/28$,

$$2\tau_5^{\text{MD}} = 2 \binom{q}{6} \frac{203 \cdot 2^n}{(2^n - q + 1)^6} \leq \frac{q^6}{2^{5n}}.$$

Using $1 \leq q \leq 2^n/28$ and applying $\sqrt{x+y} \leq \sqrt{x} + \sqrt{y}$ gives

$$\sqrt{\Gamma_5^{\text{MD}}(q, n)} \leq \frac{4q}{2^{3n/2}} + \frac{6q^2}{2^{2n}} + \frac{12q^3}{2^{5n/2}} + 6\sqrt{n} \left(\frac{q}{2^n}\right)^{3/2}.$$

Substitution gives the list forgery bound for $\mathcal{D}$. Maximizing over adversaries satisfying Equation (11) and applying Proposition 2 and Lemma 2 yield Equation (39), after simplification using $1 \leq q \leq 2^n/28$. $\square$

6 Birthday Forgery Attack and MAC Security of $F_{B_2}^{\text{EDMD}}$

6.1 Birthday Forgery Attack Against $F_{B_2}^{\text{EDMD}}$

In this subsection, we view $\mathbb{F}_2^n$ as the finite field $\mathbb{F}_{2^n}$. Take $\mathcal{M} := (\mathbb{F}_{2^n})^2$ and $h_\alpha(x, y) := \alpha x \oplus \alpha^2 y$ for $\alpha \leftarrow_{\$} \mathbb{F}_{2^n}$. This family is $2/2^n$ -AXU, as shown in Lemma 15 below. For $n \geq 64$, put $r := \lceil \sqrt{64n 2^n} \rceil$. The adversary $\mathcal{A}_{\text{bf}}$ fixes $2r$ distinct nonces and obtains tags U_i for $(N_i^{(0)}, M_0)$ and V_j for $(N_j^{(1)}, M_1)$, where $i, j \in [r]$, $M_0 := (0, 0)$, and $M_1 := (1, 0)$. Here 0 and 1 denote the zero and multiplicative identity of $\mathbb{F}_{2^n}$, respectively.

For $u \in \mathbb{F}_{2^n}$, let $m_U(u) := |\{i : U_i = u\}|$ and define m_V analogously. For each $\beta \in \mathbb{F}_{2^n}$, define

$$S_\beta := |\{(i, j) \in [r]^2 : U_i \oplus V_j = \beta, m_U(U_i) = m_V(V_j) = 1\}|.$$

Among all β maximizing S_β , let $\hat{\alpha}$ be the smallest one with respect to a fixed total order on $\mathbb{F}_{2^n}$. Let $M^*(\beta) := (\beta, 1)$. The adversary submits $(N_1^{(0)}, M^*(\hat{\alpha}), U_1)$ to Vrfy . The query is fresh since $M^*(\hat{\alpha}) = (\hat{\alpha}, 1) \neq M_0$. If $\hat{\alpha} = \alpha$, then $h_\alpha(M^*(\alpha)) = \alpha^2 \oplus \alpha^2 = 0 = h_\alpha(M_0)$, so the query is accepted.

Theorem 3 (Birthday forgery attack against $F_{B_2}^{\text{EDMD}}$). *Consider $F_{B_2}^{\text{EDMD}}$ instantiated with the hash family defined above. For $n \geq 64$, the deterministic nonce-respecting MAC adversary $\mathcal{A}_{\text{bf}}$ makes $q = 2\lceil \sqrt{64n 2^n} \rceil$ authentication queries and one verification query, and satisfies*

$$\text{Adv}_{F_{B_2}^{\text{EDMD}}}^{\text{mac}}(\mathcal{A}_{\text{bf}}) > \frac{1}{42}.$$

We prove this theorem below.

Let **Real** denote the MAC experiment for the adversary $\mathcal{A}_{\text{bf}}$ defined above, and let **Forge** be the event that its verification query is accepted.

Lemma 15. *The family $\{h_\alpha\}_{\alpha \in \mathbb{F}_{2^n}}$ is $2/2^n$ -AXU.*

Proof. For two distinct messages, let $(\Delta x, \Delta y) \neq (0, 0)$ be their difference. For any $c \in \mathbb{F}_{2^n}$, the prescribed hash difference is equivalent to

$$\Delta y \alpha^2 \oplus \Delta x \alpha = c.$$

This is a nonzero polynomial equation of degree at most two, so it has at most two roots. Since α is uniform, its probability is at most $2/2^n$. $\square$

Pair probabilities For $i, j \in [r]$ and $\beta \in \mathbb{F}_{2^n}$, define the event

$$E_{ij}(\beta) := \{U_i \oplus V_j = \beta\}.$$

Write

$$X_i := P_1(N_i^{(0)}), \quad R_j := P_1(N_j^{(1)}) \oplus \alpha.$$

So the corresponding tags satisfy

$$U_i = P_2(X_i) \oplus X_i, \quad V_j = P_2(R_j) \oplus R_j \oplus \alpha.$$

And we have

$$E_{ij}(\beta) = \{P_2(X_i) \oplus P_2(R_j) = X_i \oplus R_j \oplus \alpha \oplus \beta\}. \quad (69)$$

In the rest of this subsection, we fix $a \in \mathbb{F}_{2^n} \setminus \{0\}$.

Lemma 16. *For every $i, j \in [r]$,*

$$\frac{2}{2^n} \leq \Pr_{\text{Real}}[E_{ij}(a) \mid \alpha = a] = \frac{2^{n+1} - 3}{(2^n - 1)^2} \leq \frac{3}{2^n}. \quad (70)$$

Proof. Since the two nonces are distinct, $P_1(N_i^{(0)}) \oplus P_1(N_j^{(1)})$ is uniform over $\mathbb{F}_{2^n} \setminus \{0\}$. Thus $\Pr_{\text{Real}}[X_i = R_j \mid \alpha = a] = 1/(2^n - 1)$. On $\{\alpha = a, X_i = R_j\}$, the event $E_{ij}(a)$ holds. On $\{\alpha = a, X_i \neq R_j\}$, Equation (69) requires

$$P_2(X_i) \oplus P_2(R_j) = X_i \oplus R_j \neq 0.$$

For every fixed pair of distinct inputs, the difference of their P_2 outputs is uniform over the $2^n - 1$ nonzero values. Conditioning on whether $X_i = R_j$ gives

$$\Pr_{\text{Real}}[E_{ij}(a) \mid \alpha = a] = \frac{1}{2^n - 1} + \frac{2^n - 2}{(2^n - 1)^2} = \frac{2^{n+1} - 3}{(2^n - 1)^2},$$

which lies between $2/2^n$ and $3/2^n$. $\square$

Lemma 17. Assume $n \geq 6$.

(i) For any two distinct pairs $(i, j) \neq (i', j')$,

$$\Pr_{\text{Real}}[E_{ij}(a) \cap E_{i'j'}(a) \mid \alpha = a] \leq \frac{9}{2^{2n}}. \quad (71)$$

(ii) Fix $\beta \neq a$ and k pairs $(i_1, j_1), \dots, (i_k, j_k)$ with distinct first indices and distinct second indices. If $k^2 \leq 2^{n/2}/2$, then

$$\Pr_{\text{Real}} \left[\bigcap_{\ell=1}^k E_{i_\ell j_\ell}(\beta) \mid \alpha = a \right] \leq 3 \cdot 2^{-kn}. \quad (72)$$

Proof. Let I_0 and I_1 be the sets of first and second indices occurring in the selected pairs, and put $m_0 := |I_0| + |I_1|$. All authentication queries are fixed in advance, so the P_1 outputs at these m_0 distinct nonces are uniform over the $(2^n)_{m_0}$ injective tuples, independently of α . The values $(X_i)_{i \in I_0}$ are pairwise distinct, as are $(R_j)_{j \in I_1}$. Their cross-group equalities therefore form a partial matching. For each partial matching $J \subseteq I_0 \times I_1$, put $u := |J|$ and define

$$\mathcal{E}_J := \left\{ \begin{array}{ll} X_i = R_j & \text{for } (i, j) \in J, \\ X_i \neq R_j & \text{for } (i, j) \in (I_0 \times I_1) \setminus J \end{array} \right\}.$$

These events partition the sample space. On $\mathcal{E}_J$, exactly u cross-group pairs coincide, leaving $m_0 - u$ distinct inputs to P_2 .

For $\alpha = a$, each equality in $\mathcal{E}_J$ requires $P_1(N_i^{(0)}) = P_1(N_j^{(1)}) \oplus a$ for $(i, j) \in J$. Once the outputs at all second-group nonces and unmatched first-group nonces are chosen, the other u outputs are determined. Dropping the inequalities in $\mathcal{E}_J$ and counting the at most $(2^n)_{m_0-u}$ injective choices for these $m_0 - u$ outputs gives

$$\Pr_{\text{Real}}[\mathcal{E}_J \mid \alpha = a] \leq \frac{(2^n)_{m_0-u}}{(2^n)_{m_0}} \leq (2^n - m_0 + 1)^{-u}. \quad (73)$$

Proof of (i). Here $I_0 = \{i, i'\}$, $I_1 = \{j, j'\}$, and $m_0 \in \{3, 4\}$. There are at most $\sum_{u=0}^2 \binom{2}{u}^2 u! = 7$ partial matchings J . Fix a value $(\alpha, P_1) = (a, p_1)$ realizing $\mathcal{E}_J$. The $m_0 - u$ distinct inputs to P_2 are now fixed. By Equation (69), each selected pair corresponding to x, y requires $P_2(y) = P_2(x) \oplus x \oplus y$. Before identifying equal inputs, the two pairs form a forest with m_0 vertices and $m_0 - 2$ connected components. Identifying the u pairs in J cannot increase the number of components. Choosing one P_2 output in each component determines all outputs in that component. Hence at most $m_0 - 2$ outputs can be chosen freely, and

$$\Pr_{\text{Real}}[E_{ij}(a) \cap E_{i'j'}(a) \mid \alpha = a, P_1 = p_1] \leq \frac{(2^n)_{m_0-2}}{(2^n)_{m_0-u}} \leq (2^n - m_0 + u + 1)^{-(2-u)}.$$

Averaging the conditional bound over P_1 , summing over the partition $(\mathcal{E}_J)_J$, and using Equation (73) and $m_0 \leq 4$ yields

$$\begin{aligned} \Pr_{\text{Real}}[E_{ij}(a) \cap E_{i'j'}(a) \mid \alpha = a] &\leq \sum_J \frac{\Pr_{\text{Real}}[\mathcal{E}_J \mid \alpha = a]}{(2^n - m_0 + |J| + 1)^{2-|J|}} \\ &\leq \frac{7}{(2^n - 3)^2} < \frac{9}{2^{2n}}. \end{aligned}$$

Proof of (ii). The claim is immediate for $k = 0$, so assume $k \geq 1$. Here $I_0 = \{i_1, \dots, i_k\}$, $I_1 = \{j_1, \dots, j_k\}$, and $m_0 = 2k$. Put $D := 2^n - 2k + 1$. By Equation (73),

$$\Pr_{\text{Real}}[\mathcal{E}_J \mid \alpha = a] \leq D^{-u}.$$

If $(i_\ell, j_\ell) \in J$ for some ℓ , then on $\{\alpha = a\}$ the event $E_{i_\ell j_\ell}(\beta)$ requires $0 = a \oplus \beta$. Since $\beta \neq a$, we may omit all such J .

Fix a value $(\alpha, P_1) = (a, p_1)$ realizing a remaining $\mathcal{E}_J$. Identify the equal inputs specified by J and form the multigraph whose $2k - u$ vertices are the distinct inputs to P_2 and whose k edges are the selected pairs. Every vertex has degree at most two. There are no loops, so each component is a path or a cycle, with two parallel edges allowed as a cycle of length two. Let c be the number of cycle components. Every cycle vertex is formed by a matching pair in J , so each cycle uses at least two of the u pairs and $c \leq u/2$. For each edge joining x and y , Equation (69) requires

$$P_2(y) = P_2(x) \oplus x \oplus y \oplus a \oplus \beta.$$

Delete one edge from each cycle. The remaining $k - c$ edges form a forest with $k - u + c$ components. After choosing one output in each component, these edges determine all other outputs. Dropping the deleted equations and counting the injective output tuples of P_2 therefore gives

$$\begin{aligned} \Pr_{\text{Real}} \left[\bigcap_{\ell=1}^k E_{i_\ell j_\ell}(\beta) \mid \alpha = a, P_1 = p_1 \right] &\leq \frac{(2^n)_{k-u+c}}{(2^n)_{2k-u}} \\ &\leq (D + u)^{-(k-c)} \leq D^{-k+u/2}. \end{aligned}$$

There are at most $\binom{k}{u}^2 u! \leq k^{2u}$ matchings J of size u . Averaging the conditional bound over P_1 and summing over J gives

$$\Pr_{\text{Real}} \left[\bigcap_{\ell=1}^k E_{i_\ell j_\ell}(\beta) \mid \alpha = a \right] \leq D^{-k} \sum_{u=0}^k \left(\frac{k^2}{\sqrt{D}} \right)^u.$$

Since $2k - 1 \leq k^2 \leq 2^{n/2}/2 \leq 2^n/16$, we have $D \geq 15 \cdot 2^n/16$ and $k^2/\sqrt{D} < 3/5$. Moreover,

$$D^{-k} = 2^{-kn} \left(\frac{2^n}{D} \right)^k, \quad k \log \frac{2^n}{D} \leq \frac{k(2k-1)}{D} \leq \frac{16}{15 \cdot 2^{n/2}} \leq \frac{2}{15}.$$

Thus $D^{-k} < 6 \cdot 2^{-kn} / 5$ since $e^{2/15} < 6/5$. Therefore,

$$D^{-k} \sum_{u=0}^k \left(\frac{k^2}{\sqrt{D}} \right)^u < \frac{6}{5} 2^{-kn} \sum_{u \geq 0} \left(\frac{3}{5} \right)^u = 3 \cdot 2^{-kn}.$$

□

Completing the proof

Proof (of Theorem 3). Fix $n \geq 64$ and take r as defined above. Put

$$\lambda := \frac{r^2}{2^n}, \quad t := \left\lfloor \frac{4}{3} \lambda \right\rfloor.$$

A lower bound on $\Pr_{\text{Real}}[S_a \geq t \mid \alpha = a]$. Fix $a \in \mathbb{F}_{2^n} \setminus \{0\}$ and let

$$C_a := \sum_{i,j \in [r]} \mathbf{1}_{E_{ij}(a)}$$

count all pairs satisfying $U_i \oplus V_j = a$, including those with repeated tags. By Lemma 16, $\mathbb{E}_{\text{Real}}[C_a \mid \alpha = a] \geq 2\lambda$. If such a pair (i, j) is not counted by S_a , then $U_i = U_{i'}$ for some $i' \neq i$ or $V_j = V_{j'}$ for some $j' \neq j$. These equalities imply $E_{i'j}(a)$ and $E_{ij'}(a)$, respectively. Hence

$$C_a - S_a \leq \sum_{i,j \in [r]} \sum_{i' \neq i} \mathbf{1}_{E_{ij}(a) \cap E_{i'j}(a)} + \sum_{i,j \in [r]} \sum_{j' \neq j} \mathbf{1}_{E_{ij}(a) \cap E_{ij'}(a)}.$$

Taking conditional expectations given $\alpha = a$ and using Equation (71) gives

$$\mathbb{E}_{\text{Real}}[C_a - S_a \mid \alpha = a] \leq \frac{18r^2(r-1)}{2^{2n}} < 18 \frac{r}{2^n} \lambda.$$

Since $\lambda \geq 64n \geq 1$, expanding C_a^2 and applying Equations (70) and (71) to equal and distinct pairs, respectively, gives

$$\mathbb{E}_{\text{Real}}[C_a^2 \mid \alpha = a] \leq \frac{3r^2}{2^n} + \frac{9r^2(r-1)}{2^{2n}} \leq 12\lambda^2.$$

For $n \geq 64$, the inequality $64n \leq 2^{n/2}$ gives

$$\frac{r}{2^n} \leq \sqrt{\frac{64n}{2^n}} + 2^{-n} \leq 2^{-n/4} + 2^{-n} < \frac{1}{180}.$$

Combining this bound with the preceding estimates yields

$$\mathbb{E}_{\text{Real}}[S_a \mid \alpha = a] \geq \frac{19}{10} \lambda, \quad \mathbb{E}_{\text{Real}}[S_a^2 \mid \alpha = a] \leq 12\lambda^2.$$

By Cauchy–Schwarz,

$$\begin{aligned}\mathbb{E}_{\text{Real}}[S_a \mid \alpha = a] &= \mathbb{E}_{\text{Real}}[S_a \mathbf{1}_{\{S_a < t\}} \mid \alpha = a] + \mathbb{E}_{\text{Real}}[S_a \mathbf{1}_{\{S_a \geq t\}} \mid \alpha = a] \\ &\leq t + \sqrt{\mathbb{E}_{\text{Real}}[S_a^2 \mid \alpha = a] \Pr_{\text{Real}}[S_a \geq t \mid \alpha = a]}.\end{aligned}$$

Using $t \leq 4\lambda/3$, we obtain

$$\begin{aligned}\Pr_{\text{Real}}[S_a \geq t \mid \alpha = a] &\geq \frac{(\mathbb{E}_{\text{Real}}[S_a \mid \alpha = a] - t)^2}{\mathbb{E}_{\text{Real}}[S_a^2 \mid \alpha = a]} \\ &\geq \frac{((19/10)\lambda - (4/3)\lambda)^2}{12\lambda^2} > \frac{1}{40}.\end{aligned}\tag{74}$$

Upper bounds for $\beta \neq a$. Fix $\beta \neq a$ and put $k := 16n$. The pairs counted by S_β form a matching: two such pairs sharing a first index would have equal V tags, contrary to their uniqueness, and the same argument applies to a shared second index. The falling factorial $(S_\beta)_k$ counts ordered k -tuples of distinct pairs counted by S_β . For $n \geq 64$, we have $k^2 = 256n^2 \leq 2^{n/2}/2$. Thus, dropping the tag-uniqueness conditions in this count and applying Equation (72) gives

$$\begin{aligned}\mathbb{E}_{\text{Real}}[(S_\beta)_k \mid \alpha = a] &\leq \sum_{\substack{i_1, \dots, i_k \in [r] \text{ distinct} \\ j_1, \dots, j_k \in [r] \text{ distinct}}} \Pr_{\text{Real}} \left[\bigcap_{\ell=1}^k E_{i_\ell j_\ell}(\beta) \mid \alpha = a \right] \\ &\leq 3(r)_k^2 2^{-kn} \leq 3\lambda^k.\end{aligned}$$

Markov's inequality together with $t - k + 1 \geq 13\lambda/12$ implies

$$\begin{aligned}\Pr_{\text{Real}}[S_\beta \geq t \mid \alpha = a] &= \Pr_{\text{Real}}[(S_\beta)_k \geq (t)_k \mid \alpha = a] \\ &\leq \frac{\mathbb{E}_{\text{Real}}[(S_\beta)_k \mid \alpha = a]}{(t)_k} \\ &\leq 3 \left(\frac{\lambda}{t - k + 1} \right)^k \leq 3 \left(\frac{12}{13} \right)^k.\end{aligned}$$

A union bound over $\beta \neq a$ yields

$$\Pr_{\text{Real}}[\exists \beta \neq a : S_\beta \geq t \mid \alpha = a] \leq 3 \cdot 2^n \left(\frac{12}{13} \right)^k < \frac{1}{1000}.\tag{75}$$

Success probability. On $\{S_a \geq t\} \cap \bigcap_{\beta \neq a} \{S_\beta < t\}$, the unique maximizer is a , so $\hat{\alpha} = a$. Therefore Equations (74) and (75) give

$$\Pr_{\text{Real}}[\hat{\alpha} = a \mid \alpha = a] > \frac{1}{40} - \frac{1}{1000} = \frac{3}{125}.$$

This bound holds for every $a \neq 0$. Averaging over the nonzero hash keys gives

$$\text{Adv}_{F_{B_2}^{\text{EDMD}}}^{\text{mac}}(\mathcal{A}_{\text{bf}}) = \Pr_{\text{Real}}[\text{Forge}] \geq \Pr_{\text{Real}}[\alpha \neq 0, \hat{\alpha} = \alpha] > \left(1 - \frac{1}{2^n}\right) \frac{3}{125} > \frac{1}{42}.$$

□

6.2 Birthday MAC Security of $F_{B_2}^{\text{EDMD}}$

We next prove the following MAC-security bound.

Theorem 4 (Birthday MAC security of $F_{B_2}^{\text{EDMD}}$). *Let $n \geq 1$ and $1 \leq q < 2^n$. Then*

$$\text{Adv}_{F_{B_2}^{\text{EDMD}}}^{\text{mac}}(q, v) \leq v\varepsilon + \frac{vq\varepsilon}{2^n} + \frac{(n+2)v}{2^n - q} + \frac{q^2}{2^n}. \quad (76)$$

We also use the reduction in Section 3 to prove Theorem 4. For the list forgery advantage, we first reduce it to the probability of an event **Link**. We then compare the joint (h, P_1, Q_q) distributions in the real experiment and an auxiliary experiment **Rnd**, and bound the probability of **Link** in **Rnd**. Finally, combining these bounds proves the theorem.

Lemma 18. *For $1 \leq q < 2^n$ and $v \geq 1$,*

$$\delta_{F_{B_2}^{\text{EDMD}}}(q, v) \leq \frac{(n+1)v}{2^n - q + 1}. \quad (77)$$

Proof. Writing $x := P_1(N_i)$, for fixed h and P_2 , the $F_{B_2}^{\text{EDMD}}$ tag map for a message M is $x \mapsto P_2(x \oplus h(M)) \oplus x$. It differs from the **EWCDMD** tag map only by the fixed output offset $h(M)$, so the same bound on the number of preimages of each tag applies. The **EWCDMD** argument in the proof of Lemma 2 therefore gives Equation (77). $\square$

It remains to bound the list forgery advantage. By Section 3, it suffices to consider a deterministic, adaptive, nonce-respecting adversary $\mathcal{D}$ satisfying Equation (11). Let **Real** denote its list forgery experiment instantiated with $F_{B_2}^{\text{EDMD}}$. For $i \in [q]$, put

$$Y_i := P_1(N_i) \oplus h(M_i), \quad Z_i := T_i \oplus P_1(N_i).$$

Here Y_i is the root of the i -th authentication query, and $Z_i = P_2(Y_i)$ in **Real**.

If verification candidate j is accepted and $P_1(N'_j) \oplus h(M'_j) = Y_i$, then

$$P_1(N'_j) \oplus P_1(N_i) = h(M'_j) \oplus h(M_i) = T'_j \oplus T_i.$$

Conversely, these equalities imply that candidate j has root Y_i and is accepted. Define

$$\text{Link} := \{\exists i \in [q], j \in [v] : P_1(N'_j) \oplus P_1(N_i) = h(M'_j) \oplus h(M_i) = T'_j \oplus T_i\}.$$

Proposition 20. *If $1 \leq q < 2^n$, then*

$$\text{Adv}_{F_{B_2}^{\text{EDMD}}}^{\text{list-forg}}(\mathcal{D}) \leq \frac{v}{2^n - q} + \Pr_{\text{Real}}[\text{Link}].$$

Proof. Define the event

$$\text{NR} := \left\{ \exists j \in [v] : \begin{array}{l} P_1(N'_j) \oplus h(M'_j) \notin \{Y_1, \dots, Y_q\}, \\ T'_j = P_2(P_1(N'_j) \oplus h(M'_j)) \oplus P_1(N'_j) \end{array} \right\}.$$

By the definitions of these events, in **Real** we have

$$\text{Forge} = \text{Link} \cup \text{NR}.$$

Fix a value (h, P_1, Q_q) having positive probability in **Real**, which determines the verification list. Let m be the number of distinct authentication roots. The transcript fixes m input-output pairs of P_2 . At a new root, the output of P_2 is uniform among $2^n - m$ unused values, and acceptance specifies at most one of them. Therefore, a union bound over the verification candidates with new roots gives

$$\Pr_{\text{Real}}[\text{NR} \mid h, P_1, Q_q] \leq \frac{v}{2^n - m} \leq \frac{v}{2^n - q}.$$

Averaging and applying a union bound to the decomposition of **Forge** proves the claim. $\square$

We introduce an auxiliary authentication experiment **Rnd**, identical to **Real** except for the authentication oracle. **Rnd** first samples (h, P_1) as in **Real** but answers every authentication query with an independent uniform tag. Thus, in **Rnd**, the authentication transcript is independent of (h, P_1) .

Proposition 21. *If $1 \leq q < 2^n$, then*

$$\Delta(\mathcal{L}_{\text{Real}}(h, P_1, Q_q), \mathcal{L}_{\text{Rnd}}(h, P_1, Q_q)) \leq \frac{q(q-1)}{2^n - 1}.$$

To prove this proposition, define the event

$$\text{Good} := \{Y_i \neq Y_j, Z_i \neq Z_j \text{ for all } 1 \leq i < j \leq q\}.$$

We call a value (h, P_1, Q_q) good if it satisfies these inequalities.

Lemma 19. *For every good value (h, P_1, Q_q) having positive probability in **Rnd**,*

$$\frac{\Pr_{\text{Real}}[(\mathbf{h}, \mathbf{P}_1, \mathbf{Q}_q) = (h, P_1, Q_q)]}{\Pr_{\text{Rnd}}[(\mathbf{h}, \mathbf{P}_1, \mathbf{Q}_q) = (h, P_1, Q_q)]} = \frac{2^{nq}}{(2^n)_q} \geq 1.$$

Proof. In **Rnd**, the authentication tags are independent and uniform, so

$$\Pr_{\text{Rnd}}[\mathbf{Q}_q = Q_q \mid h, P_1] = \frac{1}{2^{nq}}.$$

Since (h, P_1, Q_q) is good, the constraints $\mathbf{P}_2(Y_i) = Z_i$ for $i \in [q]$ have pairwise distinct inputs and pairwise distinct outputs. Thus, in **Real**,

$$\Pr_{\text{Real}}[\mathbf{Q}_q = Q_q \mid h, P_1] = \Pr_{\text{Real}}[\mathbf{P}_2(Y_i) = Z_i \text{ for all } i \in [q] \mid h, P_1] = \frac{1}{(2^n)_q}.$$

The sampling probabilities of $\mathbf{h}$ and $\mathbf{P}_1$ are the same in both experiments, so taking the ratio proves the claim. $\square$

Lemma 20.

$$\Pr_{\text{Rnd}}[\neg \text{Good}] \leq \frac{q(q-1)}{2^n - 1}.$$

Proof. First fix a value (h, Q_q) having positive probability in Rnd . For $i < j$, the difference $P_1(N_i) \oplus P_1(N_j)$ is uniform over the $2^n - 1$ nonzero values, so

$$\Pr_{\text{Rnd}}[Y_i = Y_j \mid h, Q_q] = \Pr_{\text{Rnd}}[P_1(N_i) \oplus P_1(N_j) = h(M_i) \oplus h(M_j) \mid h, Q_q] \leq \frac{1}{2^n - 1}.$$

A union bound followed by averaging over (h, Q_q) gives

$$\Pr_{\text{Rnd}}[\exists i < j : Y_i = Y_j] \leq \frac{\binom{q}{2}}{2^n - 1}. \quad (78)$$

Next fix a value Q_q having positive probability in Rnd . A similar argument gives

$$\Pr_{\text{Rnd}}[\exists i < j : Z_i = Z_j] \leq \frac{\binom{q}{2}}{2^n - 1}. \quad (79)$$

The complement of **Good** is contained in the union of the two events in Equations (78) and (79). $\square$

Proof (of Proposition 21). Let

$$P := \mathcal{L}_{\text{Real}}(h, P_1, Q_q), \quad Q := \mathcal{L}_{\text{Rnd}}(h, P_1, Q_q).$$

By Lemma 19, $P(\tau) \geq Q(\tau)$ on **Good**. Therefore the positive part formula for statistical distance gives

$$\Delta(P, Q) = \sum_{\tau: Q(\tau) > P(\tau)} (Q(\tau) - P(\tau)) \leq Q(\neg \text{Good}).$$

Apply Lemma 20. $\square$

We next bound the probability of **Link** in Rnd .

Proposition 22. *If $n \geq 1$,*

$$\Pr_{\text{Rnd}}[\text{Link}] \leq v\varepsilon \left(1 + \frac{q-1}{2^n - 1} \right).$$

Proof. Fix Q_q having positive probability in Rnd . The verification list is fixed, while h and P_1 remain independent with their original distributions. For $i \in [q]$ and $j \in [v]$, put $d := T'_j \oplus T_i$. The equalities defining **Link** for this pair are

$$P_1(N'_j) \oplus P_1(N_i) = d, \quad h(M'_j) \oplus h(M_i) = d.$$

If $N'_j = N_i$, the first equality forces $d = 0$. Freshness gives $M'_j \neq M_i$, so AXU bounds the probability of the second equality by ε . In this case, for a fixed j ,

there is at most one such i . If $N'_j \neq N_i$ and $M'_j = M_i$, the two equalities are incompatible. If both the nonce and message differ, AXU and independence give

$$\Pr_{\text{Rnd}}[P_1(N'_j) \oplus P_1(N_i) = d, h(M'_j) \oplus h(M_i) = d \mid Q_q] \leq \frac{\varepsilon}{2^n - 1}.$$

Thus, conditional on $Q_q = Q_q$ and for a fixed $j \in [v]$, if $N'_j \in \{N_1, \dots, N_q\}$, the probability that candidate j satisfies the defining equalities of **Link** for some i is at most

$$\varepsilon + \frac{(q-1)\varepsilon}{2^n - 1}.$$

If $N'_j \notin \{N_1, \dots, N_q\}$, the probability is at most $q\varepsilon/(2^n - 1)$ and is no larger. A union bound over j and averaging over Q_q prove Proposition 22. $\square$

Proof (of Theorem 4). Since **Link** is determined by (h, P_1, Q_q) , we have

$$\Pr_{\text{Real}}[\text{Link}] \leq \Pr_{\text{Rnd}}[\text{Link}] + \Delta(\mathcal{L}_{\text{Real}}(h, P_1, Q_q), \mathcal{L}_{\text{Rnd}}(h, P_1, Q_q)).$$

By Propositions 20 to 22, we obtain a bound on the list forgery advantage for $\mathcal{D}$. Taking the maximum over $\mathcal{D}$ and applying Equations (12) and (77) gives

$$\text{Adv}_{F_{B_2}^{\text{mac}}}^{\text{mac}}(q, v) \leq \frac{v}{2^n - q} + \frac{q(q-1)}{2^n - 1} + v\varepsilon \left(1 + \frac{q-1}{2^n - 1}\right) + \frac{(n+1)v}{2^n - q + 1}.$$

Using $q < 2^n$ to simplify gives Equation (76). $\square$

7 Use of Generative AI Tools

OpenAI ChatGPT was used as an auxiliary research tool during the development of several parts of this work. The substantive uses relevant to the technical results are summarized below. The interactions were iterative and included many follow-up questions, reformulations, and verification steps. We therefore report representative prompts that materially contributed to the development of the final arguments, rather than the complete conversational history.

EW C Real–Clr comparison. ChatGPT was used to explore possible probabilistic descriptions of the conditional root distribution and approaches for comparing the Real and Clr experiments. A representative substantive prompt (translated from Chinese) was:

Now follow your proposed approach to prove the corresponding $5n/6$ -bit security bound, focusing on the root posterior, local switching, and per-step χ^2 or stopped-KL methods. The mathematical derivations must be rigorous; for claims that are difficult to prove, first search for counterexamples.

The resulting suggestion provided an approach for carrying out the Real–Clr comparison and were independently checked by the authors. Incorrect or unnecessarily strong intermediate claims were discarded, and the final switching argument and all quantitative bounds were derived, verified, and formalized by the authors.

EWCDMD Real-Clr_{MD} comparison. ChatGPT was used to explore the treatment of root collisions, the new-root branch, and possible Fourier-analytic approaches to the conditional tag distribution. A representative substantive prompt (translated from Chinese) was:

Refer to the draft proof of $5n/6$ -bit security for EWC in “Sources” and examine whether this approach can help prove a bound establishing $5n/6$ -bit security for EWCDMD.

The authors independently verified all probabilistic identities, moment bounds, Fourier estimates, and constants appearing in the final proof, and rewrote the argument in its final form.

Birthday forgery attack against $F_{B_2}^{\text{EDMD}}$. ChatGPT was used to investigate whether $F_{B_2}^{\text{EDMD}}$ could achieve beyond-birthday security and to explore candidate forgery strategies. A representative substantive prompt (translated from Chinese) was:

Now try to prove an upper bound establishing beyond-birthday security for the $F_{B_2}^{\text{EDMD}}$ construction.

This line of investigation led to the birthday forgery attack presented in this paper. The final attack was independently analyzed by the authors, including its success probability, query complexity, and parameter conditions.

Tool information and author verification. The authors used OpenAI ChatGPT with the GPT-5.5, GPT-5.6 Sol, and GPT-6 Astra models during July–September 2026. AI outputs were treated as suggestions rather than authoritative results. All mathematical statements, proofs, calculations, references, and attack arguments included in the final manuscript were independently checked and revised by the authors. The authors take full responsibility for all content and results in the paper.

References

1. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: *Advances in Cryptology – EUROCRYPT 2006*. Lecture Notes in Computer Science, vol. 4004, pp. 409–426. Springer (2006), <https://eprint.iacr.org/2004/331>
2. Brassard, G.: On computationally secure authentication tags requiring short secret shared keys. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) *Advances in Cryptology: Proceedings of CRYPTO 82*. pp. 79–86. Plenum Press, New York (1983). https://doi.org/10.1007/978-1-4757-0602-4_7
3. Chen, Y.L., Mennink, B., Preneel, B.: Categorization of faulty nonce misuse resistant message authentication. In: *Advances in Cryptology – ASIACRYPT 2021, Part III*. Lecture Notes in Computer Science, vol. 13092, pp. 520–550. Springer (2021). https://doi.org/10.1007/978-3-030-92078-4_18, <https://eprint.iacr.org/2021/1696>

4. Choi, W., Inoue, A., Lee, B., Lee, J., List, E., Minematsu, K., Naito, Y.: Highly secure nonce-based MACs from the sum of tweakable block ciphers. *IACR Trans. Symm. Cryptol.* **2020**(4), 39–70 (2020). <https://doi.org/10.46586/tosc.v2020.i4.39-70>
5. Choi, W., Lee, B., Lee, Y., Lee, J.: Improved security analysis for nonce-based enhanced hash-then-mask MACs. In: Moriai, S., Wang, H. (eds.) *ASIACRYPT 2020*, Part I. LNCS, vol. 12491, pp. 697–723. Springer, Cham (Dec 2020). https://doi.org/10.1007/978-3-030-64837-4_23
6. Choi, W., Lee, J., Lee, Y.: Toward full n-bit security and nonce misuse resistance of block cipher-based MACs. In: Chung, K.M., Sasaki, Y. (eds.) *ASIACRYPT 2024*, Part IX. LNCS, vol. 15492, pp. 251–279. Springer, Singapore (Dec 2024). https://doi.org/10.1007/978-981-96-0947-5_9
7. Cogliati, B., Dutta, A., Nandi, M., Patarin, J., Saha, A.: Proof of mirror theory for a wide range of $\xi_{\max}$. In: *Advances in Cryptology – EUROCRYPT 2023*, Part IV. Lecture Notes in Computer Science, vol. 14007, pp. 470–501. Springer (2023). https://doi.org/10.1007/978-3-031-30634-1_16, <https://eprint.iacr.org/2022/686>
8. Cogliati, B., Seurin, Y.: EWCDM: An efficient, beyond-birthday secure, nonce-misuse resistant MAC. In: *Advances in Cryptology – CRYPTO 2016*, Part I. Lecture Notes in Computer Science, vol. 9814, pp. 121–149. Springer (2016). https://doi.org/10.1007/978-3-662-53018-4_5, <https://eprint.iacr.org/2016/525>
9. Cover, T.M., Thomas, J.A.: *Elements of Information Theory*. Wiley-Interscience, Hoboken, NJ, 2 edn. (2006). <https://doi.org/10.1002/047174882X>
10. Csiszár, I., Körner, J.: *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2 edn. (2011). <https://doi.org/10.1017/CB09780511921889>
11. Dai, W., Hoang, V.T., Tessaro, S.: Information-theoretic indistinguishability via the chi-squared method. In: *Advances in Cryptology – CRYPTO 2017*, Part III. Lecture Notes in Computer Science, vol. 10403, pp. 497–523. Springer (2017)
12. Datta, N., Dutta, A., Dutta, K.: Improved security bound of (E/D)WCDM. *IACR Trans. Symm. Cryptol.* **2021**(4), 138–176 (2021). <https://doi.org/10.46586/tosc.v2021.i4.138-176>
13. Datta, N., Dutta, A., Nandi, M., Yasuda, K.: Encrypt or decrypt? To make a single-key beyond birthday secure nonce-based MAC. In: Shacham, H., Boldyreva, A. (eds.) *CRYPTO 2018*, Part I. LNCS, vol. 10991, pp. 631–661. Springer, Cham (Aug 2018). https://doi.org/10.1007/978-3-319-96884-1_21
14. Dinur, I.: Tight indistinguishability bounds for the XOR of independent random permutations by fourier analysis. In: *Advances in Cryptology – EUROCRYPT 2024*, Part I. Lecture Notes in Computer Science, vol. 14651, pp. 33–62. Springer (2024). https://doi.org/10.1007/978-3-031-58716-0_2, <https://eprint.iacr.org/2024/338>
15. Dinur, I.: Combining outputs of a random permutation: New constructions and tight security bounds by fourier analysis. In: *Advances in Cryptology – EUROCRYPT 2025*, Part I. Lecture Notes in Computer Science, vol. 15601, pp. 244–273. Springer (2025). https://doi.org/10.1007/978-3-031-91107-1_9, <https://eprint.iacr.org/2024/929>
16. Dutta, A., Nandi, M., Talnikar, S.: Beyond birthday bound secure MAC in faulty nonce model. In: *Advances in Cryptology – EUROCRYPT 2019*, Part I. Lecture Notes in Computer Science, vol. 11476, pp. 437–466. Springer (2019)
17. Gibbs, A.L., Su, F.E.: On choosing and bounding probability metrics. *International Statistical Review* **70**(3), 419–435 (2002). <https://doi.org/10.1111/j.1751-5823.2002.tb00178.x>

18. Handschuh, H., Preneel, B.: Key-recovery attacks on universal hash function based MAC algorithms. In: *Advances in Cryptology – CRYPTO 2008*. Lecture Notes in Computer Science, vol. 5157, pp. 144–161. Springer (2008)
19. Hoeffding, W.: Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association* **58**(301), 13–30 (1963). <https://doi.org/10.1080/01621459.1963.10500830>
20. Joux, A.: Authentication failures in NIST version of GCM. Comments submitted to the NIST Modes of Operation Process (2006), https://csrc.nist.gov/csrc/media/projects/block-cipher-techniques/documents/bcm/joux_comments.pdf
21. Mennink, B., Neves, S.: Encrypted Davies–Meyer and its dual: Towards optimal security using mirror theory. In: *Advances in Cryptology – CRYPTO 2017, Part III*. Lecture Notes in Computer Science, vol. 10403, pp. 556–583. Springer (2017). https://doi.org/10.1007/978-3-319-63697-9_19, <https://eprint.iacr.org/2017/473>
22. Nandi, M.: Mind the composition: Birthday bound attacks on EWCDMD and SoKAC21. In: *Advances in Cryptology – EUROCRYPT 2020, Part I*. Lecture Notes in Computer Science, vol. 12105, pp. 203–220. Springer (2020). https://doi.org/10.1007/978-3-030-45721-1_8, <https://eprint.iacr.org/2020/236>
23. O’Donnell, R.: *Analysis of Boolean Functions*. Cambridge University Press (2014). <https://doi.org/10.1017/CB09781139814782>
24. Patarin, J.: The “coefficients H” technique (invited talk). In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) *SAC 2008*. LNCS, vol. 5381, pp. 328–345. Springer, Berlin, Heidelberg (Aug 2009). https://doi.org/10.1007/978-3-642-04159-4_21
25. Patarin, J.: Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography. *Cryptology ePrint Archive*, Report 2010/287 (2010), <https://eprint.iacr.org/2010/287>
26. Shoup, V.: On fast and provably secure message authentication based on universal hashing. In: *Advances in Cryptology – CRYPTO ’96*. Lecture Notes in Computer Science, vol. 1109, pp. 313–328. Springer (1996)
27. Wegman, M.N., Carter, J.L.: New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences* **22**(3), 265–279 (1981). [https://doi.org/10.1016/0022-0000\(81\)90033-7](https://doi.org/10.1016/0022-0000(81)90033-7)