Parallelizable MACs Based on the Sum of PRPs with Security Beyond the Birthday Bound

Alexander Moch[1] and Eik List[2]

[1] Universität Mannheim, Mannheim, Germany
<lastname>(at)uni-mannheim.de

[2] Bauhaus-Universität Weimar, Weimar, Germany
<firstname>.<lastname>(at)uni-weimar.de

Abstract. The combination of universal hashing and encryption is a fundamental paradigm for the construction of symmetric-key MACs, dating back to the seminal works by Wegman and Carter, Shoup, and Bernstein. While fully sufficient for many practical applications, the Wegman-Carter construction, however, is well-known to break if nonces are ever repeated, and provides only birthday-bound security if instantiated with a permutation. Those limitations inspired the community to several recent proposals that addressed them, initiated by Cogliati et al.'s Encrypted Wegman-Carter Davies-Meyer (EWCDM) construction.

This work extends this line of research by studying two constructions based on the sum of PRPs: (1) a stateless deterministic scheme that uses two hash functions, and (2) a nonce-based scheme with one hash-function call and a nonce. We show up to $2n/3$-bit security for both of them if the hash function is universal. Compared to the EWCDM construction, our proposals avoid the fact that a single reuse of a nonce can lead to a break.

Keywords: Symmetric-key cryptography · authentication · provable security · permutation · beyond-birthday security · pseudorandom function · universal hashing.

1 Introduction

Message Authentication Codes (MACs) aim to guarantee the authenticity and integrity of submitted messages. So, a receiver can successfully determine with high probability whether a given pair (m, t) of message and tag has been generated by the legitimate sender and has been transmitted correctly or not. MACs can be stateless deterministic, randomized, stateful; in general, one also distinguishes nonce-based constructions where the sender is responsible to supply a unique nonce to each message to be authenticated. Since cryptographically secure randomness can be expensive to obtain in various settings, our focus is on stateless and nonce-based constructions, hereafter.

While the primary goal of a MAC is unforgeability, indistinguishability from random bits can be a valuable replacement goal to evaluate the security. If tags are indistinguishable from random, they are also hard to forge.

The Wegman-Carter approach [35] is a popular and efficient paradigm for constructing secure MACs. There, a given message is first compressed with a universal hash function before the result is processed by a cryptographically secure random function. The initial approach added the hash $h_{k'}(m)$ of a given message m to a key stream k to create a tag: $t = h_{k'}(m) \oplus k$; in practice, the key stream is supposed to be computed from some secure pseudorandom function $F(\nu)$ from some nonce ν. In [34], Shoup replaced the function F with a permutation, addressing the fact that there exist a number of standardized and well-analyzed block ciphers. Bernstein later proved the security of Shoup's construction, e.g., [3]. Bernstein's well-known bound still ensures that the advantage for any adversary that asks $2^{n/2}$ authentication queries [2] is bounded by $1.7 q_v \ell / 2^n$, where q_v is the number of verification queries and ℓ is the maximal message length, usually in terms of elements of a ring or field used in h. Throughout this work, we adopt the common way of referring to security bounds that are negligible up to $\mathcal{O}(2^{n/2})$ blocks or queries as $n/2$ bits of security.

Despite its simplicity, one can identify two interesting directions of extending the Wegman-Carter construction. The first concerns the nonce requirement, which is a well-known considerable risk: If a single nonce is repeated only once, the security of the construction may collapse completely since the hash-function key could leak. Secondly, even if nonces never repeat, its security is inherently limited by Bernstein's bound, which is of birthday-bound type. Recent works showed that Bernstein's bound is tight [22,28], which means that the original construction cannot provide higher security.

An ongoing series of research aims to find constructions with higher security guarantees that retained some security also under nonce reuse. As one of the starting points, one could identify the proposal of the Encrypted Davies-Meyer (EDM) and the Encrypted Wegman-Carter Davies-Meyer (EWCDM) modes by Cogliati et al. [9]. While EDM is a PRP-to-PRF conversion method and therefore restricted to inputs of n bits length, EWCDM supports nonce-based authentication for variable-input-length messages as does the original Wegman-Carter construction. In EWCDM, a nonce ν is first processed by the Davies-Meyer construction under a permutation π_1; its result is XORed with the hash of a message m and the sum is encrypted under a second independent permutation: $\pi_2(\pi_1(\nu) \oplus \nu \oplus h_{k'}(m))$. EDM misses the hash and uses ν as the only message input. Its authors showed that both constructions provide at least $2n/3$-bit security. Recently, Cogliati and Seurin [10] showed that one can use the same permutation twice in EDM while retaining $2n/3$-bit security.

Mennink and Neves [24] improved on EWCDM. They proved almost full (i.e., n-bit) security for EDM and EWCDM and they further proved the full n-bit security of a newly proposed dual, EDMD and EWCDMD. As a side effect, they made Patarin's Mirror Theory [30,31,32] easier to grasp for a broader audience. Although Nandi [27] pointed out a slip in [24], which meant that the security of the nonce-based version of its dual, EWCDMD, is still limited by the birthday bound, the work by Mennink and Neves opened the gates for a wider study of possible constructions. At CRYPTO'18, Datta et al. [13] extended this direction of research by the Decrypted Wegman-Carter Davies-Meyer construction (DWCDM), a single-key variant of EWCDM that employs the permutation in both directions. The maximal security of their construction was capped by $2n/3$ bits by design.

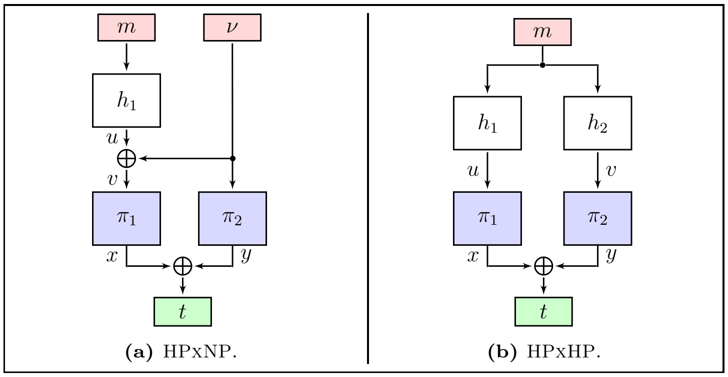
An alternative approach has been taken by Cogliati et al. [8]. They proposed four generic constructions based on the composition of universal hashing and a block cipher: Hash-as-Tweak (HaT), Nonce-as-Tweak (NaT), Hash-as-Key (HaK), and Nonce-as-Key (NaK). They proved n-bit security for all constructions in the ideal-permutation model (assuming a universal hash function). However, the former two constructions require a tweakable primitive, whereas the latter two require message-dependent rekeying.

We can identify four desiderata for interesting MACs based on permutations and universal hashing. In terms of security, the adversary's advantage should remain negligible for $\ell q \gg 2^{n/2}$. In terms of simplicity, the number of calls to the primitive(s) should be minimized. For efficiency, their calls should be parallelizable, and frequent rekeying should be avoided. Last but not least, they should support variable-length messages. So, inspite of recent advances, it remains an interesting question how one can generally achieve those aspects for stateless deterministic and/or nonce-based constructions.

Contribution. This work analyzes two constructions based on permutations and universal hashing with the help of the Mirror Theory. Our first construction is stateless deterministic whereas our second is nonce-based. We name them HPxNP and HPxHP, according to the fact whether they employ a universal hash function (HP) or a nonce (NP) as inputs to the permutation. Figure 1 illustrates them schematically. We show that both modes provide $\mathcal{O}(2n/3)$ bits of security asymptotically.

Outline. Hereupon, we first cover briefly the necessary preliminaries used in this work, including a brief recap of Patarin's Mirror Theory. Thereupon, Section 3 proposes our three constructions whose security is then analyzed in the subsequent Sections 4 and 5. Section 6 concludes.

Remark 1. We note that the HPxHP construction is clearly not novel, but an abstraction of a variety of existing double-lane MACs, e.g., 3kf9 [38], GCM-SIV-2 [19], or PMAC$^+$ [37]. However, in its abstract form, it has been studied by Datta et al. [11] (the same authors already had studied the construction in [12]) from a constructive view; in parallel to our work, Dutta et al. also analyzed a variant of HPxNP with a single bit for domain separation in [16], where they also showed $O(q^3/2^{2n})$ bits of security. Recently, Leurent et al. [21] also studied an attacking view. More precisely, Leurent et al. [21] proposed a forgery attack with data complexity of $\mathcal{O}(2^{3n/4})$ for such constructions. We also take the constructive view, so that our derived security bound is also inherently limited by the result by Leurent et al.; moreover, at the end of each analysis section, we further discuss the effect of using 4-wise independent hash functions for our constructions, with the positive result that the then-obtained security bounds render their result inapplicable and lead to higher security.



(a) HPxNP. **(b)** HPxHP.

Fig. 1: Our proposed constructions. π_1 and π_2 represent two permutations over $\{0,1\}^n$, h_1 and h_2 two universal hash functions, m a variable-length message, ν, ν^1, and ν^2 nonces of fixed length, and t the authentication tag.

2 Preliminaries

General Notations. We use calligraphic uppercase letters $\mathcal{X}, \mathcal{Y}$ for sets. We write $\{0,1\}^n$ for the set of bit strings of length n, and denote the concatenation of binary strings x and y by $x \parallel y$ and the result of their bitwise XOR by $x \oplus y$. We write $x \twoheadleftarrow \mathcal{X}$ to mean that x is chosen uniformly at random from the set $\mathcal{X}$. We consider $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$ to be the set of all deterministic mappings $F : \mathcal{X} \to \mathcal{Y}$ and $\mathsf{Perm}(\mathcal{X})$ to be the set of all permutations over $\mathcal{X}$. Given an event E, we denote by $\Pr[E]$ the probability of E. For two integers n, k with $n \geq k \geq 1$, we denote the falling factorial as $(n)_k \overset{\text{def}}{=} \prod_{i=0}^{k-1}(n-i)$.

A (complexity-theoretic) distinguisher $\mathbf{A}$ is an efficient adversary, i.e., an efficient Turing machine that is given access to a number of oracles $\mathcal{O}$ which it can interact with. The task of $\mathbf{A}$ is to distinguish between two worlds of oracles, one of which is chosen at the beginning of the experiment uniformly at random. After its interaction, $\mathbf{A}$ outputs a bit that represents a guess of the world that $\mathbf{A}$ interacted with. The distinguishing advantage between a real world $\mathcal{P}$ and an ideal world $\mathcal{O}$ is given by $\Delta_{\mathbf{A}}(\mathcal{P}, \mathcal{O}) \overset{\text{def}}{=} \left|\Pr\left[\mathbf{A}^{\mathcal{P}} \Rightarrow 1\right] - \Pr\left[\mathbf{A}^{\mathcal{O}} \Rightarrow 1\right]\right|$. Throughout this work, we consider information-theoretic distinguishers, i.e., distinguishers that are computationally unbounded, and that are limited only by the number of queries they can ask to their available oracles. We assume that distinguishers do not ask duplicate queries or queries to which they already can compute the answer themselves from earlier queries, as is common. W.l.o.g., we limit our interest to deterministic distinguishers since for each probabilistic distinguisher, there exists a deterministic one with equal advantage that fixed a random tape beforehand (cf. [1,7]).

We briefly recall the definitions for the advantage of distinguishing a construction from a random function (PRF) and from a random permutation (PRP), respectively.

Definition 1 (PRF Advantage). Let $\mathcal{K}$, $\mathcal{X}$, and $\mathcal{Y}$ be non-empty sets and let $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ and $\rho \twoheadleftarrow \mathsf{Func}(\mathcal{X}, \mathcal{Y})$ and $k \twoheadleftarrow \mathcal{K}$. Then, the PRF advantage of $\mathbf{A}$ w.r.t. F is defined as $\mathbf{Adv}_F^{\mathrm{PRF}}(\mathbf{A}) \overset{\mathrm{def}}{=} \Delta_{\mathbf{A}}(F_k, \rho)$.

A keyed permutation $E : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$ is a family of permutation over $\mathcal{X}$ indexed by a key $K \in \mathcal{K}$.

Definition 2 (PRP Advantage). Let $\mathcal{K}$ and $\mathcal{X}$ be non-empty sets, $E : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$ be a keyed permutation, and let $\pi \twoheadleftarrow \mathsf{Perm}(\mathcal{X})$ and $k \twoheadleftarrow \mathcal{K}$. Then, the PRP advantage of $\mathbf{A}$ w.r.t. F is defined as $\mathbf{Adv}_{E_k}^{\mathrm{PRP}}(\mathbf{A}) \overset{\mathrm{def}}{=} \Delta_{\mathbf{A}}(E_k, \pi)$.

To recall the necessary definitions for universal hashing, let $\mathcal{X}$ and $\mathcal{Y}$ denote two non-empty sets, and $\mathcal{H} = \{h : \mathcal{X} \to \mathcal{Y}\}$ be a family of hash functions h.

Definition 3 (Almost-Universal Hash Function [5]). We say that $\mathcal{H}$ is ε-almost-universal (ε-AU) if, for all distinct $x, x' \in \mathcal{X}$, it holds that $\Pr_{h \twoheadleftarrow \mathcal{H}}[h(x) = h(x')] \leq \varepsilon$.

Almost-XOR-universal hash functions were introduced in [20]; the term, however, is due to Rogaway [33].

Definition 4 (Almost-XOR-Universal Hash Function [20,33]). Here, let $\mathcal{Y} \subseteq \{0,1\}^n$ for some positive integer n. We say that $\mathcal{H}$ is ε-almost-XOR-universal (ε-AXU) if, for all distinct $x, x' \in \mathcal{X}$ and arbitrary $\Delta \in \mathcal{Y}$, it holds that $\Pr_{h \twoheadleftarrow \mathcal{H}}[h(x) \oplus h(x') = \Delta] \leq \varepsilon$.

Definition 5 (k-wise Independence [36]). We say that $\mathcal{H}$ is k-independent if, for all pair-wise distinct $x_1, \ldots x_k \in \mathcal{X}$ and all $y_1, \ldots, y_k \in \mathcal{Y}^k$, it holds that $\Pr_{h \twoheadleftarrow \mathcal{H}}[h(x_i) = y_i, \text{ for } 1 \leq i \leq k] = 1/|\mathcal{Y}|^k$.

2.1 H-coefficient Technique

The H-coefficients technique is a proof method due to Patarin, where we consider the variant by Chen and Steinberger [7,29]. The results of the interaction of an adversary $\mathbf{A}$ with its oracles are collected in a transcript τ. The oracles can sample randomness prior to the interaction (often a key or an ideal primitive that is sampled beforehand), and are then deterministic throughout the experiment [7]. The task of $\mathbf{A}$ is to distinguish the real world $\mathcal{O}_{\mathrm{real}}$ from the ideal world $\mathcal{O}_{\mathrm{ideal}}$. Let Θ_{real} and Θ_{ideal} denote the distribution of transcripts in the real and the ideal world, respectively. A transcript τ is called *attainable* if the probability to obtain τ in the ideal world – i.e. over Θ_{ideal} – is non-zero. Then, the fundamental Lemma of the H-coefficients technique, the proof to which is given in [7,29], states:

Lemma 1 (Fundamental Lemma of the H-coefficient Technique [29]). Assume, the set of attainable transcripts can be partitioned into two disjoint sets GoodT and BadT. Further assume that there exist $\epsilon_1, \epsilon_2 \geq 0$ such that for any transcript $\tau \in \mathsf{GoodT}$, it holds that

$$\frac{\Pr[\Theta_{\mathrm{real}} = \tau]}{\Pr[\Theta_{\mathrm{ideal}} = \tau]} \geq 1 - \epsilon_1, \quad \text{and} \quad \Pr[\Theta_{\mathrm{ideal}} \in \mathsf{BadT}] \leq \epsilon_2.$$

Then, for all adversaries $\mathbf{A}$, it holds that $\Delta_{\mathbf{A}}(\mathcal{O}_{\mathrm{real}}, \mathcal{O}_{\mathrm{ideal}}) \leq \epsilon_1 + \epsilon_2$.

2.2 Mirror Theory

We will combine the H-coefficient technique with Patarin's Mirror Theory, which allows us to lower bound the amount of good transcripts. Taking the ratio yields then the probability to obtain a good transcript. In the following, we briefly recall the necessary definitions according to the Mirror Theory according to [24] that followed Patarin [30,31].

Remark 2. Mirror Theory became popular to a broader audience after its reformulation by Mennink and Neves [24]. While the core ideas are not difficult to understand, the proof by Patarin in [30] employed a recursive argument that has been subject to intensive debates in the past, cf. [13,24]. The correctness of the argument for the first recursion has been established, where Patarin showed $\mathcal{O}(2n/3)$ bits of security for the sum of permutations [30]. Patarin's proof had to approximate the second recursion; a full proof would have to continue on for many further recursions with an exponentional number of cases, which seems a highly sophisticated task. Clearly, it is out of scope of this work.

Instead of relying on the assumptions of the full Mirror Theory, we follow the line of e.g., [13,23] and consider it not for full n-bit security. In this work, we require only up to $\mathcal{O}(2n/3)$ bits of security, thus, effectively relying only the first recursion.

Mirror theory evaluates the number of possible solutions to a system of affine equations of the form $P_{a_i} \oplus P_{b_i} = \lambda_i$ in a finite group. Let $q \geq 1$ denote a number of equations and $r \geq 1$ a number of unknowns. Let $\mathcal{P} = \{P_1, \ldots, P_r\}$ represent the set of r distinct unknowns and consider an equation system

$$\mathcal{E} = \left\{ P_{a_1} \oplus P_{b_1} = \lambda_1, \ldots, P_{a_q} \oplus P_{b_q} = \lambda_q \right\},$$

where a_i, b_i for $1 \leq i \leq q$ are mapped to $\{1, \ldots, r\}$ by a surjective index mapping $\varphi : \{a_1, b_1, \ldots, a_q, b_q\} \to \{1, \ldots, r\}$. Given a subset of equations $\mathcal{I} \subseteq \{1, \ldots, q\}$, the multiset $\mathcal{M}_{\mathcal{I}}$ is defined as $\mathcal{M}_{\mathcal{I}} = \bigcup_{i \in \mathcal{I}} \{\varphi(a_i), \varphi(b_i)\}$.

Definition 6 (Circle-freeness). An equation system $\mathcal{E}$ is circle-free if there exists no subset of indices $\mathcal{I} \subseteq \{1, \ldots, q\}$ of equations s.t. $\mathcal{M}_{\mathcal{I}}$ has even multiplicity elements only.

So, no linear combination of equations is independent of the unknowns.

Definition 7 (Block-maximality). Let $\mathcal{Q}_1, \ldots, \mathcal{Q}_s = \{1, \ldots, r\}$ be a partitioning of the r indices into s minimal so-called blocks s.t. for all equation indices $i \in \{1, \ldots, q\}$, there exists a single block index $\ell \in \{1, \ldots, s\}$ s.t. the unknowns of the i-th equation are contained in only this block: $\{\varphi(a_i), \varphi(b_i)\} \subseteq \mathcal{Q}_\ell$. Then, the system of equations $\mathcal{E}$ is called ξ-block-maximal for $\xi \geq 2$ if there exists no $i \in \{1, \ldots, s\}$ s.t. $|\mathcal{Q}_i| > \xi$.

So, the unknowns can be partitioned into blocks of size at most $\xi + 1$ if $\mathcal{E}$ is ξ-block-maximal.

Definition 8 (Non-degeneracy). A system of equations $\mathcal{E}$ is non-degenerate iff there is no $\mathcal{I} \subseteq \{1, \ldots, q\}$ s.t. $\mathcal{M}_{\mathcal{I}}$ has exactly two odd multiplicity elements and $\bigoplus_{i \in \mathcal{I}} \lambda_i = 0$.

So, an equation system is non-degenerate if there is no linear combination of one or more equations that imply $P_i = P_j$ for distinct i, j and $P_i, P_j \in \mathcal{P}$. The central theorem of Patarin's mirror theorem is then Theorem 2 in [24], which itself is a brief form of Theorem 6 in [30].

Theorem 1 (Mirror Theorem [24]). *Let $\xi \geq 2$. Let $\mathcal{E}$ be a system of equations over the unknowns $\mathcal{P}$ that is (i) circle-free, (ii) ξ-block-maximal, and (iii) non-degenerate. Then, as long as $(\xi - 1)^2 \cdot r \leq 2^n/67$, the number of solutions s.t. $P_i \neq P_j$ for all pairwise distinct $i, j \in \{1, \ldots, r\}$ is at least*

$$\frac{(2^n)_r}{(2^n)^q}.$$

A proof sketch is given in [24, Appendix A], and the details in [30]. An updated proof had been given in [26].

Mennink and Neves described a relaxation wherein the condition that two unknowns P_a and P_b must differ whenever a and b differ is released to the degree that distinct unknowns must be pairwise distinct only inside their blocks. So, it must hold for $a \neq b$ that $P_a \neq P_b$ when $a, b \in \mathcal{R}_j$ for some $j \in \{1, \ldots, s\}$ for a given partitioning $\{1, \ldots, r\} = \bigcup_{i=1}^{s} \mathcal{R}_i$.

Definition 9 (Relaxed Non-degeneracy). An equation system $\mathcal{E}$ is relaxed non-degenerate w.r.t. the partitioning $\{1, \ldots, r\} = \bigcup_{i=1}^{s} \mathcal{R}_i$ iff there is no $\mathcal{I} \subseteq \{1, \ldots, q\}$ s.t. $\mathcal{M}_{\mathcal{I}}$ has exactly two odd multiplicity elements and $\bigoplus_{i \in \mathcal{I}} \lambda_i = 0$.

In [24, Theorem 3], Mennink and Neves extend Theorem 1 to the following relaxed form:

Theorem 2 (Relaxed Mirror Theorem [24]). *Let $\xi \geq 2$ and let $\{1, \ldots, r\} = \bigcup_{i=1}^{s} \mathcal{R}_i$ be a partition of the r indices. Let $\mathcal{E}$ be a system of equations over the unknowns $\mathcal{P}$ that is (i) circle-free, (ii) ξ-block-maximal, and (iii) non-degenerate w.r.t. the partition $\{1, \ldots, r\}$. Then, as long as $(\xi - 1)^2 \cdot r \leq 2^n/67$, the number of solutions s.t. $P_i \neq P_j$ for all pairwise distinct $i, j \in \{1, \ldots, r\}$ is at least*

$$\frac{\mathsf{NonEq}(\mathcal{R}_1, \ldots, \mathcal{R}_s; \mathcal{E})}{(2^n)^q},$$

where $\mathsf{NonEq}(\mathcal{R}_1, \ldots, \mathcal{R}_s; \mathcal{E})$ is the number of solutions to $\mathcal{P}$ that satisfy $P_a \neq P_b$ for all $a, b \in \mathcal{R}_j$ for all $1 \leq j \leq s$ as well as all inequalities (the equalities released) by $\mathcal{E}$.

Mennink and Neves stress that the relaxed Theorem 2 is equivalent to Theorem 1 for $s = 1$, i.e., when the equation system consists of a single block. Moreover, the number of solutions that are covered in the term $\mathsf{NonEq}(\mathcal{R}_1, \ldots, \mathcal{R}_s; \mathcal{E})$ can be lower bounded by $(2^n)_{|\mathcal{R}_1|} \cdot \prod_{i=2}^{s} (2^n - (\xi - 1))_{|\mathcal{R}_i|}$ since every variable is in exactly one block which imposes at most $\xi - 1$ additional inequalities to the other unknowns in its block.

Remark 3. We consider PRF security in the information-theoretic setting, similar as [24]. The underlying permutations are secret and assumed to be drawn uniformly at random from $\mathsf{Perm}(\{0,1\}^n)$. Our results generalize to the complexity-theoretic setting. There, the permutations π_1 and π_2 are supposed to be instantiated with a block cipher E under independent random secret keys k_1 and k_2, E_{k_1} and E_{k_2}, respectively. The bounds from this paper can be easily adapted to the complexity-theoretic setting by adding a term of $2 \cdot \mathbf{Adv}^{\mathrm{PRP}}_{E_k}(q)$. The term refers to twice the maximal advantage for an adversary $\mathbf{A}'$ to distinguish $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ keyed with a random key $k \twoheadleftarrow \mathcal{K}$ from a random permutation π, where $\mathbf{A}$ asks at most q queries. Note that we only employ the forward direction of the permutation; therefore, PRP security suffices and we do not need to consider the strong variant.

3 Constructions

Let $n \geq 1$ be a positive integer, and let $\mathcal{K}$ denote a non-empty set. Let $\pi_1, \pi_2 \twoheadleftarrow \mathsf{Perm}(\{0,1\}^n)$ be independently uniformly at random sampled permutations over n-bit strings. Let $\mathcal{H} = \{h \mid h : \{0,1\}^* \to \{0,1\}^n\}$ be a family of ε_1-AXU hash functions; for HPxHP, we will define and use instead $\mathcal{H}_1 = \{h_1 \mid h_1 : \{0,1\}^* \to \{0,1\}^n\}$ be a family of ε_1-AU hash functions, and $\mathcal{H}_2 = \{h_2 \mid h_2 : \{0,1\}^* \to \{0,1\}^n\}$ be a family of ε_2-AU hash functions. We require the hash functions to be sampled independently uniformly at random. Usually, the hash function instances are determined by sampling a hash key independently uniformly at random for each instance.

Our first, nonce-based construction, HPxNP, is illustrated in Figure 1a. It shares similarities with Minematsu's Enhanced Hash-then-Mask construction [25] that had been analyzed further in [14,15]; however, Minematsu's construction used a function instead of a permutation and a per-message random IV. In this construction, the message is hashed to an n-bit value $h(m)$. For this construction, we need $\mathcal{H}$ to be an ε-almost-XOR-universal family of hash functions. An n-bit nonce ν is XORed to the hash u to obtain $v := h(m) \oplus \nu$; v and ν serve as inputs to the two calls to a permutation π_1 and π_2, respectively, and yield $x := \pi_1(v)$ and $y := \pi_2(\nu)$. Finally, the outputs of the permutation calls are XORed and released as authentication tag: $t := x \oplus y$.

Our second construction, HPxHP, is illustrated in Figure 1b. It consists of two parallel invocations of the hash functions on the input message $m \in \{0,1\}^*$ that are hashed using $h_1 \in \mathcal{H}_1$ and $h_2 \in \mathcal{H}_2$, respectively, to two n-bit values u and v. Those serve as inputs to the two calls to a permutation π_1 and π_2, respectively and yield $x := \pi_1(u)$ and $y := \pi_2(v)$. Finally, the outputs of the permutation calls are XORed and released as authentication tag: $t := x \oplus y$.

In practice, the permutations π_1 and π_2 will be instantiated with a secure block cipher E under two independent keys k_1 and k_2. An intuitive choice for the hash function is, for example, polynomial hashing. Let $\mathbb{F}_{2^n}$ be the Galois Field $GF(2^n)$ with a fixed primitive polynomial $p(\mathtt{x})$. For $n = 128$, the GCM polynomial $p(\mathtt{x}) = \mathtt{x}^{128} + \mathtt{x}^7 + \mathtt{x}^2 + \mathtt{x} + \mathtt{1}$ is a usual choice. The hash function is instantiated by sampling a hash key $k \twoheadleftarrow \mathbb{F}_{2^n}$. Given k and a message $m \in (\mathbb{F}_{2^n})^\ell$ of ℓ blocks, polynomial hashing is then defined as the sum of

$$h_k(m) \overset{\text{def}}{=} \sum_{i=1}^{\ell} k^{\ell+1-i} \cdot m_i,$$

where m_i denotes the i-th message block and additions as well as multiplications are in $\mathbb{F}_{2^n}$.

It is well-known that for maximal message lengths of ℓ blocks (after padding), polynomial hashing is ε-AXU for $\varepsilon = \ell/2^n$, and therefore also $\ell/2^n$-AU. Note that polynomial hashing requires an injective padding to prevent trivial hash collisions; a simple 10^*-padding works, but may extend messages by one block.

While the sum of a polynomial hash is sequential, computing the individual terms on a few cores in parallel is well-known at the cost of storing multiple powers of the hash key. For instance, optimized instances of GCM parallelize the computations of four (or eight) subsequent blocks $k^4 \cdot m_i$, $k^3 \cdot m_{i+1}$, $k^2 \cdot m_{i+2}$, and $k^4 \cdot m_{i+3}$, before their results are summed, reduced by the modulus, and summed to the sum of the previous blocks $\sum_{j=1}^{i-1} k^j m_j$ [17,18]. Thus, several hash multiplications, or two hash-function calls, or hashing and computing a permutation are efficiently parallelizable as long as the platform is not too resource-restricted. Note that a number of related hash functions exist with similar security properties; pseudo-dot-product hashing, BRW hashing, or combined approaches such as [6] can half the number of necessary multiplications, and provide similar parallelizability. We refer the interested reader to an overview by Bernstein [4].

4 Security Analysis of HPxNP

First, we consider the construction HPxNP. Patarin's approach [30] allows us to obtain a bound of $\mathcal{O}(2n/3)$ bits of security. At the end of this section, we discuss the implications of considering ξ_{average} instead, as was also suggested ibidem.

Theorem 3. Let $n \geq 1, \xi \geq 2$ be integers, and $\mathcal{H} = \{h \,|\, h : \{0,1\}^* \to \{0,1\}^n\}$ be a family of ε-AXU hash functions with $h \twoheadleftarrow \mathcal{H}$. For any nonce-respecting PRF distinguisher $\mathbf{A}$ that asks at most $q \leq 2^n/(67\xi^2)$ queries, it holds that

$$\mathbf{Adv}^{\text{PRF}}_{\text{HPxNP}[h,\pi_1,\pi_2]}(\mathbf{A}) \leq \frac{2q^2 \cdot \varepsilon}{\xi^2} + \frac{\binom{q}{2} \cdot \varepsilon}{2^n} + \frac{q}{2^n}.$$

Note that in this case, the optimal choice of ξ to obtain the best bound is $2^{n/6}$, assuming that $\varepsilon \in \mathcal{O}(2^{-n})$. Then, the bound in Theorem 3 is dominated by the first term of $\mathcal{O}(q^2/2^{4n/3} + q^2/2^{2n} + q/2^n)$, while the number of queries is allowed to be $q \leq 2^{2n/3}$. Other values for ξ reduce either the security bound or the number of queries.

The remainder of this section is devoted to show Theorem 3. Here, $\mathbf{A}$ makes q construction queries (ν_i, m_i), for $1 \leq i \leq q$, that are stored together with the query results t_i in a transcript $\tau = \{(\nu_i, m_1, t_1), \ldots, (\nu_q, m_q, t_q)\}$. In both worlds, the oracle samples h at the beginning uniformly at random from all hash instances. $\mathbf{A}$ sees the results t_i after each query. We employ a common method to alleviate the proof: after the adversary finished its interaction with the oracle, but before outputting its final decision bit, $\mathbf{A}$ is given the hash-function instance h so that it can compute the values $u_1, \ldots, u_q$ itself. Clearly, this only makes the adversary stronger, but spares the need to discuss security internals of the hash function.

Let $1 \le r \le 2q$ and consider the set $\mathcal{P} = \{P_1, \ldots, P_r\}$ of r unknowns. We consider a system of q equations

$$\mathcal{E} = \{P_{a_1} \oplus P_{b_1} = t_1, \quad P_{a_2} \oplus P_{b_2} = t_2, \quad \ldots, \quad P_{a_q} \oplus P_{b_q} = t_q\},$$

where $P_{a_i} := x_i = \pi_1(h(m_i) \oplus \nu_i)$ and $P_{b_i} := y_i = \pi_2(\nu_i)$. We further define an index mapping $\varphi : \{a_1, b_1, \ldots, a_q, b_q\} \to \{1, \ldots, r\}$. For all $i, j \in \{1, \ldots, q\}$:

- $\varphi(a_i) \ne \varphi(a_j) \Leftrightarrow h_1(m_i) \oplus \nu_i \ne h_1(m_j) \oplus \nu_j$.
- $\varphi(b_i) \ne \varphi(b_j)$ since $\nu_i \ne \nu_j$.
- $\varphi(a_i) \ne \varphi(b_j)$ since both permutations π_1 and π_2 are independent.

The index mapping φ has a range of size $q_x + q_y$, where $q_x = |\{x_i, \ldots, x_q\}| \le q$ and $q_y = |\{\nu_1, \ldots, \nu_q\}| = q$.

4.1 Bad Transcripts

φ only exposes collisions of the form $\varphi(a_i) = \varphi(a_j)$ or equivalently $x_i = x_j$. We define the following bad events:

- bad_1: there exist ξ distinct equation indices $i_1, i_2, \ldots, i_\xi \in \{1, \ldots, q\}$ s.t. $x_{i_1} = x_{i_2} = \ldots = x_{i_\xi}$ where ξ is the threshold given in Theorem 3.
- bad_2: There exist query indices $i \ne j$, $i, j \in \{1, \ldots, q\}$ s.t. $(v_i, t_i) = (v_j, t_j)$.

Let us consider bad_1 first. Since h is ε-AXU, the expected amount of collisions is $q^2 \cdot \varepsilon$. Unfortunately ε-AXU is not strong enough to allow for statements regarding multicollisions, i.e. we cannot make a statement on the probability that three or more input values collide. Considering the maximal block size ξ, the worst case would be that all collisions occur in the same hash value. If there exists a block of size $(\xi + 1)$, this block contains ξ^2 collisions. Let $\#\mathsf{Colls}(q)$ be the random variable that counts the collisions in h. By Markov's Inequality, the probability that there are more than $\binom{\xi}{2}$ collisions in h is at most:

$$\Pr\left[\#\mathsf{Colls}_1(q) \ge \binom{\xi}{2}\right] \le \frac{\mathbb{E}(C)}{\binom{\xi}{2}} = \frac{\binom{q}{2} \cdot \varepsilon}{\binom{\xi}{2}} \le \frac{2q^2\varepsilon}{\xi^2}.$$

For bad_2, recall that the ideal world samples the tags independently uniformly at random. Since h is ε-AXU, it follows for some distinct pair $i, j \in \{1, \ldots, q\}$:

$$\Pr[v_i = v_j \wedge t_i = t_j] \le \frac{\binom{q}{2} \cdot \varepsilon}{2^n}.$$

It follows from the sum of both probability for bad_1 and bad_2 that

$$\Pr[\tau \in \mathsf{BadT}\,|\Theta_{\text{ideal}} = \tau] \le \frac{2q^2 \cdot \varepsilon}{\xi^2} + \frac{\binom{q}{2} \cdot \varepsilon}{2^n}.$$

4.2 Ratio of Good Transcripts

Lemma 2. The system of equations is (i) circle-free, (ii) ξ-block-maximal and (iii) relaxed non-degenerate with respect to the partitioning into $\mathcal{R}_1 \sqcup \mathcal{R}_2$, where $\mathcal{R}_1 =^{\text{def}} \{\varphi(a_1), \ldots, \varphi(a_q)\}$ and $\mathcal{R}_2 =^{\text{def}} \{\varphi(b_1), \ldots, \varphi(b_q)\}$.

Proof. The proof relies on the fact that $\varphi(b_i) \neq \varphi(b_j)$ and $\varphi(a_i) \neq \varphi(b_j)$ for any $i \neq j$. For any $\mathcal{I} \subseteq \{1, \ldots, q\}$ the corresponding multiset $M_{\mathcal{I}}$ has at least $|\mathcal{I}|$ odd multiplicity elements and therefore the system of equations $\mathcal{E}$ is (i) circle-free.

(ii) If $\mathcal{E}$ were not ξ-block-maximal, then there must be an ordering $\mathcal{I} = \{i_1, \ldots, i_\xi\}$ s.t. $\varphi(a_{i_1}) = \ldots = \varphi(a_{i_\xi})$. This is equivalent to a ξ-fold collision $x_{i_1} = \ldots = x_{i_\xi}$, which contradicts the assumption that τ is a good transcript.

(iii) Suppose that $\mathcal{E}$ would be relaxed degenerate. Then, there would exist a minimal subset $\mathcal{I} \subseteq 1, \ldots, q$ that has exactly two odd multiplicity elements corresponding to the same oracle and s.t. $\bigoplus_{i \in \mathcal{I}} t_i = 0$. If $|\mathcal{I}| = 1$, $M_{\mathcal{I}}$ would have two elements from different oracles. If $|\mathcal{I}| = 2$ and $t_{i_1} = t_{i_2}$, then we would know that $x_{i_1} \neq x_{i_2}$ since $\nu_{i_1} \neq \nu_{i_2}$, i.e. $y_{i_1} \neq y_{i_2}$. Therefore, we have four odd multiplicity elements. If $|\mathcal{I}| \geq 3$, there would exist at least three odd multiplicity elements. So, $\mathcal{E}$ cannot be relaxed degenerate, which concludes the proof. □

Lemma 3. Let $\tau \in \mathsf{GoodT}$ and $q \leq 2^n/(67\xi^2)$. Then, it holds that

$$\frac{\Pr\left[\Theta_{\text{real}} = \tau\right]}{\Pr\left[\Theta_{\text{ideal}} = \tau\right]} \geq 1 - \frac{q}{2^n}.$$

Proof. The probability to obtain a good transcript τ consists of that for obtaining the tags $t_1, \ldots, t_q$, and the hash-function outputs $h(m_i)$. The probability to obtain the latter is given in both worlds by $|\mathcal{H}|^{-1}$. The bound in Lemma 3 is determined by the ratio of the respective probabilities. This term appears in the real world as well as in the ideal world and cancels out eventually. Hence, we ignore it for the remainder of the analysis. The probability of obtaining the rest of the transcript, i.e., the tags t_i, in the ideal world is then given by

$$\Pr\left[t_1, \ldots, t_q \middle| \Theta_{\text{ideal}}\right] = \frac{1}{(2^n)^q}$$

since the outputs t_i are sampled independently and uniformly at random from $\{0,1\}^n$ in the ideal world. In the real world, the probability is given by

$$\begin{aligned}\Pr\left[\Theta_{\text{real}} = \tau\right] &\geq \frac{\frac{\mathsf{NonEQ}(\mathcal{R}_1, \mathcal{R}_2; \mathcal{E})}{2^{nq}} \cdot (2^n - q_x)! \cdot (2^n - q_y)!}{(2^n!)^2} \\ &= \frac{\mathsf{NonEQ}(\mathcal{R}_1, \mathcal{R}_2; \mathcal{E})}{2^{nq}(2^n)_{q_x}(2^n)_{q_y}}.\end{aligned}$$

Remember that $q_y = q$ since all ν_i are distinct. To lower bound $\mathsf{NonEQ}(\mathcal{R}_1, \mathcal{R}_2; \mathcal{E})$, note that we have $(2^n)_{q_x}$ choices for $\{P_j \mid j \in \mathcal{R}_1\}$ and at least $(2^n - 1)_q$ possible choices for $\{P_j \mid j \in \mathcal{R}_2\}$, as every index in $\mathcal{R}_2$ is in a block with exactly one unknown from $\mathcal{R}_1$. Thus

$$\Pr\left[\Theta_{\text{real}} = \tau\right] \geq \frac{(2^n-1)_q (2^n)_{q_x}}{2^{nq}(2^n)_q (2^n)_{q_x}} = \frac{1}{2^{nq}}\left(1 - \frac{q}{2^n}\right).$$

Hence, we obtain the ratio as in Lemma 3. □

4.3 Using ξ_{average}

In [30], Patarin suggests that one can potentially consider the average instead of the maximal block size for the sum of permutations in the Mirror Theory. More precisely, Generalization 2 of [30, Section 6] suggests that:

> "The theorem $P_i \oplus P_j$ is still true if we change the condition $\xi_{\max}\alpha \ll 2^n$ by $\xi_{\text{average}} \ll 2^n$."

The bottleneck in our bound is the event bad_1; bad_2 as well as the good transcripts do not consider ξ at all and the respective terms become significant only for q approaching 2^n. Upper bounding the block size is necessary to ensure the condition $q \leq 2^n/(67\xi_{\max}^2)$. Using a universal family of hash functions only allows for a very crude upper bound of the maximal block size that limits us at a security level of around $2^{2n/3}$ queries.

If we could use the average block size as suggested by Patarin, we are limited by the condition $q \leq 2^n/(67\xi_{\text{average}}^2)$; then, bad_1 would no longer be necessary and would significantly improve the bound. The following theorem would yield an upper bound on the expected average block size ξ_{average}.

Theorem 4. For any $q \leq 2^n$ and $\varepsilon \leq 1$, we expect that $\xi_{\text{average}} \leq (q-1)\varepsilon + 2$.

The proof is deferred to Appendix A, but we will briefly sketch the idea for $\varepsilon = 2^{-n}$: For $q \ll 2^n$, the expected amount of collisions $q^2/2^n$ is in $\mathcal{O}(q)$. For $q = 2^n$, the expected amount of collisions is 2^{n-1}. In the worst case (regarding the average), the collisions are uniformly distributed, i.e. $h(m_1) = h(m_2), h(m_3) = h(m_4), \ldots, h(m_{2^n-1}) = h(m_{2^n})$. This pattern corresponds to the case that every block were of size 3 and hence the average is 3 as well. Any other pattern would not increase the average block size. The proof will consider the more general case for ε. From Theorem 4, we obtain

$$q \leq \frac{2^n}{67((q-1)\varepsilon + 2)^2}.$$

We note that the use of ξ_{average} implies the need to employ the stronger form of the Mirror Theory, that assumes that the iterated proof suggested by Patarin holds. Both the stronger form of the Mirror Theory and the Generalization 2 [30] are subject to their own analysis.

5 Security Analysis of HPxHP

The analysis of HPxHP shares many similarities with that of HPxNP, but differs in certain key points. Regarding the maximum block size, a hash collision (considering the hashes separately) may occur now on one of both sides, i.e., there may be a collision in $h_1(m) = h_1(m')$ or in $h_2(m) = h_2(m')$, which increases the block size and effectively doubles the probability of obtaining a hash collision.[3] Further, since collisions may occur on both sides, it is possible to obtain a circle.

Using a universal hash function, we can obtain security up to $\mathcal{O}(2^{2n/3})$ queries, matching the security bound of earlier analyses. Increasing the strength of the hash function and using a k-wise independent hash function, it is possible to obtain security up to $\mathcal{O}(2^{\frac{(n-1)k}{k+1}})$ queries. Putting stronger requirements on the family of hash functions increases its size and therefore the length of the key. We still find this result interesting since recent results [21] provided attacks with a query complexity of $\mathcal{O}(2^{3n/4})$. If we demand stronger properties from the hash function, our security level exceeds the complexity by the known attacks. Again, we provide an analysis with a universal hash function and $\xi_{\max}$ first. Thereupon, we will argue about the necessary proof changes to adapt to stronger hash-function families.

Theorem 5. Let $n \geq 1, \xi \geq 2$ be integers and $\mathcal{H}_1$ and $\mathcal{H}_2$ be ε_1 and ε_2-AU families of hash functions, respectively, and let $h_1 \twoheadleftarrow \mathcal{H}_1$ and $h_2 \twoheadleftarrow \mathcal{H}_2$ be sampled independently uniformly at random. Let $\varepsilon =^{\text{def}} \max\{\varepsilon_1, \varepsilon_2\}$. For any PRF distinguisher $\mathbf{A}$ that asks at most $q \leq 2^n/(67\xi^2)$ queries, it holds that

$$\mathbf{Adv}^{\mathrm{PRF}}_{\mathrm{HPxHP}[h_1,h_2,\pi_1,\pi_2]}(\mathbf{A}) \leq \frac{4q^2\varepsilon}{\xi^2} + 3 \cdot (q\varepsilon)^2 + q^3\varepsilon^2 + \frac{\xi \cdot q}{2^n - \xi}.$$

For $\xi = 2^{n/6}$, and assuming an optimal $\varepsilon = \mathcal{O}(2^{-n})$, the bound in Theorem 5 has the form of $\mathcal{O}(q^2/2^{4n/3} + q^2/2^{2n} + q^3/2^{2n} + q/2^{5n/6})$ for $q \in \mathcal{O}(2^{2n/3})$ queries. So, it is dominated by the first term. The remainder of this section contains the proof of Theorem 5. Consider a deterministic distinguisher $\mathbf{A}$ that has access to either HPxHP$[h_1, h_2, \pi_1, \pi_2]$ or ρ, which chooses the outputs given to $\mathbf{A}$ uniformly at random. $\mathbf{A}$ makes q construction queries m_i that are stored together with the query results t_i in a transcript $\tau = \{(m_1, t_1), \ldots, (m_q, t_q)\}$. In both worlds, the oracle samples h_1 and h_2 at the beginning independently and uniformly at random from their hash families. $\mathbf{A}$ sees the results t_i after each query. Again, we make the adversary stronger by defining that the hash keys are revealed to the adversary after it finished its interaction with the oracle, but before outputting its final decision bit.

Let $1 \leq r \leq 2q$ and consider the set $\mathcal{P} = \{P_1, \ldots, P_r\}$ of r unknowns. Again, we consider a system of q equations

$$\mathcal{E} = \{P_{a_1} \oplus P_{b_1} = t_1, \quad P_{a_2} \oplus P_{b_2} = t_2, \quad \ldots, \quad P_{a_q} \oplus P_{b_q} = t_q\},$$

[3] Technically speaking, there is a total of $q(q-1)/2$ of input pairs. When bounding the probability of a collision we used q^2 instead, ignoring the factor 1/2.

where $P_{a_i} := x_i = \pi_1(h_1(m_i))$ and $P_{b_i} := y_i = \pi_2(h_2(m_i))$. We further define an index mapping $\varphi : \{a_1, b_1, \ldots, a_q, b_q\} \to \{1, \ldots, r\}$; φ maps equal permutation outputs $x_i = x_j$ that occur for any $i \neq j$ (from equal hash values $u_i = u_j$) to the same unknown P_k; similarly, φ maps equal permutation outputs $y_i = y_j$ that occur for any $i \neq j$ (from equal hash values $v_i = v_j$) to the same unknown P_ℓ. For all $i, j \in \{1, \ldots, q\}$, it holds that

- $\varphi(a_i) \neq \varphi(a_j) \Leftrightarrow h_1(m_i) \neq h_1(m_j)$.
- $\varphi(b_i) \neq \varphi(b_j) \Leftrightarrow h_2(m_i) \neq h_2(m_j)$.
- $\varphi(a_i) \neq \varphi(b_j)$ since both permutations π_1 and π_2 are independent.

In the real world, the transcript has collisions in the values $x_i = x_j$ or $y_i = y_j$ for $i \neq j$, when the corresponding hash values $u_i = u_j$ or $v_i = v_j$ collide. A collision in x_i and x_j corresponds to a collision in $\varphi(a_i)$ and $\varphi(a_j)$ and a collision in y_i and y_j corresponds to a collision in $\varphi(b_i)$ and $\varphi(b_j)$. Multi-collisions in the range values of π_1 and π_2 correspond to blocks in the mirror theory. To upper bound the size of the largest block $\mathcal{Q}_k$, we need to consider a special type of collision between two queries i and j. In this setting, we say that two queries i and j collide if $h_1(m_i) = h_1(m_j)$ and/or[4] $h_2(m_i) = h_2(m_j)$. The probability for such a collision to happen is $\varepsilon_1 + \varepsilon_2 \leq 2\varepsilon$.

We define an event bad_1 if there exists a ξ-multi-collision in any subset of queries $\{i_1, \ldots, i_{\xi+1}\} \subseteq \{1, \ldots, q\}$, where ξ is the threshold in Theorem 5. We need to consider four more events that render a transcript to be bad:

- bad_1: There exists a subset $\mathcal{I} \subseteq \{1, \ldots, q\}$ of size $|\mathcal{I}| = \xi$, s.t. for each pair of distinct indices $i, j \in \mathcal{I}$, it holds that $\varphi(a_i) = \varphi(a_j)$ and/or $\varphi(b_i) = \varphi(b_j)$; ξ is the threshold in Theorem 5.
- bad_2: There exist $i \neq j$, $i, j \in \{1, \ldots, q\}$ s.t. $(u_i, v_i) = (u_j, v_j)$ and $t_i \neq t_j$.
- bad_3: There exist $i \neq j$, $i, j \in \{1, \ldots, q\}$ s.t. $(u_i, t_i) = (u_j, t_j)$ and $v_i \neq v_j$.
- bad_4: There exist $i \neq j$, $i, j \in \{1, \ldots, q\}$ s.t. $(v_i, t_i) = (v_j, t_j)$ and $u_i \neq u_j$.
- bad_5: There exists a subset $\mathcal{I} \subseteq \{1, \ldots, q\}$ s.t. $\mathcal{M}_\mathcal{I}$ contains only elements of even multiplicity.

If an attainable transcript τ is not bad, we define τ as good. We denote by GoodT and BadT the sets of good and bad transcripts, respectively. In the H-coefficient technique, the probability that a transcript is bad is analyzed solely for the ideal world. The bound in Theorem 5 follows then from Lemma 1 and Lemmas 4–6.

5.1 Bad Transcripts

Lemma 4. Let $\xi \geq 1$ denote the threshold from Theorem 5. It holds that

$$\Pr\left[\tau \in \mathsf{BadT} \,|\, \Theta_{\text{ideal}} = \tau\right] \leq \frac{4q^2\varepsilon}{\xi^2} + 3 \cdot (q\varepsilon)^2 + q^3\varepsilon^2.$$

[4] To avoid confusion, by 'and/or' we actually mean the logical 'or'.

Proof. In the following, we upper bound the probability that a transcript is bad. Most of the time, we can upper bound the probabilities of the individual bad events to occur and will simply take the sum of their probabilities. We will postpone the discussion of the first bad event to the end and begin with the second bad event.

For the second bad event, it holds that h_1 and h_2 are both ε-AU and independent. We drop the condition $t_i \neq t_j$ since it only decreases the probability and an upper bound suffices for our purpose. The probability that both hash values collide simultaneously for two queries is at most

$$\Pr[\mathsf{bad}_2] \leq \binom{q}{2}\varepsilon^2 \leq \frac{q^2\varepsilon^2}{2}.$$

For the third and fourth bad events, the probabilities can be formulated similarly. To upper bound bad_3, the probability that $u_i = u_j$ is again at most ε for a fixed pair of distinct query indices $i \neq j$. Since the outputs t_i and t_j are sampled uniformly at random and independently from the hash values, we can again neglect the requirement $v_i \neq v_j$ and obtain the same upper bound for bad_3 as for bad_2 when we use $\varepsilon \geq 2^{-n}$. A similar argument holds for bad_4.

When upper bounding the probability of bad_5, we are limited by the hash function. We consider all 3-tuples (m_a, m_b, m_c) such that $h_1(m_a) = h_1(m_b)$ and $h_2(m_b) = h_2(m_c)$. This event can be bounded by $\binom{q}{3}\varepsilon^2$, which also excludes the occurrence of a circle. Thus, it holds that $\Pr[\mathsf{bad}_5] \leq q^3\varepsilon^2$. Double-collisions that are small circles by themselves are excluded by bad_2.

Now, we will consider bad_1. As in the analysis of HPxNP we will upper bound the maximal block size for the individual hash functions. We will then condition bad_1 on $\neg\mathsf{bad}_5$ to ensure that no collisions in h_1 are connected to collisions in h_2. The hash functions are both ε-almost-universal. Again, the worst case regarding block maximality would be that all collisions occur in the same block of size $\xi+1$. Such a block would have $\binom{\xi}{2}$ collisions. Let $\#\mathsf{Colls}_1(q)$ denote a random variable for the number of collisions between $h_1(m_i) = h_1(m_j)$ for $1 \leq i, j \leq q$ and $i \neq j$. Using Markov's Inequality, we obtain an upper bound for the probability that

$$\Pr\left[\#\mathsf{Colls}_1(q) \geq \binom{\xi}{2}\right] \leq \frac{\mathbb{E}[\#\mathsf{Colls}_1(q)]}{\binom{\xi}{2}} \leq \frac{2q^2\varepsilon}{\xi^2}.$$

We can derive a similar argument using a random variable $\#\mathsf{Colls}_2(q)$ for the number of collisions between collisions $h_2(m_i) = h_2(m_j)$, So, the probability to obtain a block of size ξ is upper bounded by

$$\Pr[\mathsf{bad}_1 | \neg\mathsf{bad}_5] \leq \frac{4q^2\varepsilon}{\xi^2}.$$

Our bound in Lemma 4 follows from summing up the obtained terms. □

5.2 Good Transcripts

It remains to upper bound the ratio of probabilities to obtain a good transcript in both worlds. To upper bound it in the real world, we will use the Relaxed

Mirror Theory. We show that a good transcript fulfills all the properties needed by the Relaxed Mirror Theorem.

Lemma 5. Let $\tau \in \mathsf{GoodT}$. Let $\mathcal{E}$ be the system of q equations corresponding to $(\varphi^\tau, m_1, \ldots, m_q)$. Then, $\mathcal{E}$ is (i) circle-free, (ii) ξ-block-maximal, and (iii) relaxed non-degenerate w.r.t. the partitioning $\{1, \ldots, r\} = \mathcal{R}_1 \cup \mathcal{R}_2$, where $\mathcal{R}_1 = \{\varphi(a_i), \ldots, \varphi(a_q)\}$ and $\mathcal{R}_2 = \{\varphi(b_i), \ldots, \varphi(b_q)\}$.

Proof. We defined τ to be a good transcript; hence, no bad event has occurred, which implies that the transcript is (i) circle-free since we excluded bad_5 here.

(ii) If $\mathcal{E}$ were not ξ-block-maximal, there would exist a minimal subset $\mathcal{Q} \subseteq \{1, \ldots, r\}$ with $|\mathcal{Q}| \geq \xi + 1$ so that there exists some $i \in \{1, \ldots, q\}$ for which either $\{\varphi(a_i), \varphi(b_i)\} \subseteq \mathcal{Q}$ or $\{\varphi(a_i), \varphi(b_i)\} \cap \mathcal{Q} = \emptyset$. The latter event does not violate the block-maximality, so we can focus on the former statement.

Assuming that $\mathcal{E}$ were not ξ-block-maximal, we can define a subset of indices $\mathcal{I} \subset \{1, \ldots, q\}$ for which it holds that $\{\varphi(a_i), \varphi(b_i)\} \subseteq \mathcal{Q}$ for all $i \in \mathcal{I}$. Then, we can define an ordered sequence of the indices in $\mathcal{I}$ to $i_1, \ldots, i_\xi$ s.t. it would have to hold for all pairs of subsequent indices i_j, i_{j+1}, for $1 \leq j < \xi$ that $\varphi(a_i) = \varphi(a_j)$ and/or $\varphi(b_i) = \varphi(b_j)$. This is equivalent to our definition of bad_1 and would therefore violate our assumption that τ is good. Hence, every good transcript τ is ξ-block-maximal.

(iii) Assume that τ would be relaxed degenerate. This would imply there exists a subset $\mathcal{I} \subseteq \{1, \ldots, q\}$ such that the multiset $M_{\mathcal{I}}$ has exactly two odd multiplicity elements from a single set $\mathcal{R}_1$ or $\mathcal{R}_2$ and the tags of the elements corresponding to $\mathcal{I}$ sum up to zero, i.e.

$$\bigoplus_{i \in \mathcal{I}} t_i = \bigoplus_{i \in \mathcal{I}} \pi_1(h_1(m_i)) \oplus \pi_2(h_2(m_i)) = 0.$$

Recall that $\varphi(a_i) \neq \varphi(a_j)$ if and only if $h_1(m_i) \neq h_1(m_j)$, $\varphi(b_i) \neq \varphi(b_j)$ if and only if $h_2(m_i) \neq h_2(m_j)$ and $\varphi(a_i) \neq \varphi(b_j)$ for any choice of i and j. An element $\varphi(a_i)$ has even multiplicity in $M_{\mathcal{I}}$ if there is an even amount of inputs that collide in $h_1(m_i)$. And similarly an element $\varphi(b_i)$ has even multiplicity in $M_{\mathcal{I}}$ if there is an even amount of inputs that collide in $h_2(m_i)$. If there is an even amount of queries that collide in a hash value, one can easily see that these elements will cancel out in the above sum.

For simplicity, assume, there exists a subset $\mathcal{I} \subseteq \{1, \ldots, q\}$ with exactly two odd multiplicity elements from $\mathcal{R}_1$ and even multiplicity elements only from $\mathcal{R}_2$. All elements from $\mathcal{R}_2$ cancel out in the sum above. and all even multiplicity elements from $\mathcal{R}_1$ cancel out as well. Let the two odd multiplicity elements from $\mathcal{R}_1$ have multiplicity $2n_1 + 1$ and $2n_2 + 1$, where $n_1, n_2 \geq 0$. In total, $2n_1$ and $2n_2$ terms will cancel out and what remains is $\pi_1(h_1(m_i)) \oplus \pi_1(h_1(m_j)) = 0$ where $\varphi(a_i) \neq \varphi(a_j)$. However, this event cannot occur since $\varphi(a_i) \neq \varphi(a_j)$ implies that $h_1(m_i) \neq h_1(m_j)$; thus the system cannot be relaxed degenerate. □

Lemma 6. Let $\tau \in \mathsf{GoodT}$ and $q \leq 2^n/(67\xi^2)$. Then, it holds that

$$\frac{\Pr[\Theta_{\text{real}} = \tau]}{\Pr[\Theta_{\text{ideal}} = \tau]} \geq 1 - \frac{\xi \cdot q}{2^n - \xi}.$$

Proof. The probability to obtain a good transcript τ consists of that for obtaining the tags $t_1, \ldots, t_q$, and the hash-function outputs u_i and v_i. The probability to obtain the latter is given in both worlds by $\Pr[(h_1, h_2) \mid (h_1, h_2) \twoheadleftarrow \mathcal{H}_1 \times \mathcal{H}_2]$. The bound in Lemma 6 is determined by the ratio of the respective probabilities. This term appears in the real world as well as in the ideal world and cancels out eventually. Hence, we ignore it for the remainder of the analysis. The probability for the tags t_i in the ideal world is then given by $\Pr[t_1, \ldots, t_q | \Theta_{\text{ideal}}] = 1/(2^n)^q$ since the outputs t_i are sampled independently and uniformly at random from $\{0,1\}^n$ in the ideal world.

In the real world, the situation is more complex and a little more work is necessary. We denote by $q_x := |\{\pi_1(h_1(m_i)) \mid i \in \{1, \ldots, q\}\}|$ the amount of distinct values for π_1 and similarly we denote by $q_y := |\{\pi_2(h_2(m_i)) \mid i \in \{1, \ldots, q\}\}|$ the amount of distinct values for π_2. The number of solutions to the $q_x + q_y$ unknowns is at least $\mathsf{NonEQ}(\mathcal{R}_1, \mathcal{R}_2; \mathcal{E})/2^{nq}$. There are $(2^n - q_x)!$ possible choices for the remaining output values of π_1 and $(2^n - q_y)!$ possible choices for the remaining output values of π_2. Thus, we can lower bound

$$\Pr[\Theta_{\text{real}} = \tau] \geq \frac{\frac{\mathsf{NonEQ}(\mathcal{R}_1, \mathcal{R}_2; \mathcal{E})}{2^{nq}} \cdot (2^n - q_x)! \cdot (2^n - q_y)!}{(2^n!)^2} = \frac{\mathsf{NonEQ}(\mathcal{R}_1, \mathcal{R}_2; \mathcal{E})}{2^{nq}(2^n)_{q_x}(2^n)_{q_y}}.$$

We will use the obvious lower bound for $\mathsf{NonEQ}(\mathcal{R}_1, \mathcal{R}_2; \mathcal{E})$ and we obtain

$$\Pr[\Theta_{\text{real}} = \tau] \geq \frac{(2^n)_{q_x}(2^n - \xi)_{q_y}}{2^{nq}(2^n)_{q_x}(2^n)_{q_y}} = \frac{1}{2^{nq}} \cdot \frac{(2^n - \xi)_{q_y}}{(2^n)_{q_y}}.$$

We can immediately see that

$$\frac{\Pr[\Theta_{\text{real}} = \tau]}{\Pr[\Theta_{\text{ideal}} = \tau]} \geq \frac{(2^n - \xi)_{q_y}}{(2^n)_{q_y}}.$$

We can further reformulate the expression $(2^n - \xi)_{q_y}/(2^n)_{q_y}$ to

$$\frac{(2^n - q_y)(2^n - q_y - 1) \cdots (2^n - q_y - (\xi - 1))}{(2^n)(2^n - 1)(2^n - 2) \cdots (2^n - (\xi - 1))} = \prod_{i=0}^{\xi - 1} \frac{2^n - i - q_y}{2^n - i}.$$

This can be reformed to and upper bounded by

$$\prod_{i=0}^{\xi-1} \left(1 - \frac{q_y}{2^n - i}\right) \geq \left(1 - \frac{q}{2^n - \xi}\right)^{\xi} \geq 1 - \frac{\xi \cdot q}{2^n - \xi},$$

where the final inequality is Bernoulli's. □

5.3 Using *k*-wise Independent Hash Functions

In contrast to the analysis of HPxNP, for HPxHP, we find ξ not only in the analysis of bad_1, but also in that of bad_5 plus in the bound for the good transcripts. For the same reasons as in HPxNP, bad_1 and bad_5 cap the bound at around $q = 2^{2n/3}$. Using the average block size would not work here since it would not affect the bound of bad_5. However, we can increase the security bound of HPxHP with stronger, k-wise independent hash functions. For even k, this allows to obtain a bound of $q = 2^{kn/(k+1)}$ since such hash functions yield better bounds for circles of sizes $\geq k$. Since circles always contain an even amount of queries, there would be no benefit of an uneven values k. Leurent et al. required a 4-circle that is expected after $2^{3n/4}$ queries for their attack. Using a 4-independent hash function, the first 4-circle occurs after 2^n queries on average. So, we can obtain a security bound that exceeds the complexity of Leurent et al.'s attack. For simplicity, we will consider 4-wise independent hash functions first and illustrate the changes to the security bound of HPxHP. Thereupon, we extend our analysis to larger values of k. For space limitations, we defer the proofs of Lemma 7 and 8 to Appendix C.

Lemma 7. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be independent 4-wise independent hash functions. Let $\xi \geq 7$. Then

$$\Pr\left[\mathsf{bad}_1 | \neg\mathsf{bad}_2\right] \leq \frac{2\binom{q}{4}}{2^{3n}\binom{\xi}{4}} + \frac{16q^5}{2^{4n}}.$$

We find two interesting points here: (1) Raising the requirement of the hash functions to 4-wise independence yields a 4-circle after 2^n queries on average instead of after $2^{3n/4}$ queries as in the attack by Leurent et al.. Thus, a security level of $2^{4n/5}$ can be obtained. (2) We cannot show yet if it is possible to consider ξ_{average} instead of $\xi_{\max}$. If we can consider the average block size instead of the maximum block size, the upper bound of circles is the bottleneck. Vice versa, it seems that attacks on the HPxHP-type of MACs must exploit the occurrence of circles. We can formulate the following lemma to bound the probability of bad_5.

Lemma 8. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be independent 4-wise independent hash functions. Then $\Pr\left[\mathsf{bad}_5 | \neg\mathsf{bad}_2 \wedge \neg\mathsf{bad}_1\right] \leq q^4/2^{4n}$.

6 Conclusion

We presented two MAC constructions that are provably secure to up to $\mathcal{O}(2^{2n/3})$ queries; HPxHP avoids nonces at the price of two independent hash-function evaluations; HPxNP trades one hash-function call for the use of a nonce.

Our results add to the works that demonstrate the usefulness of Patarin's Mirror Theory for such constructions. We indicated that considering the average instead of the maximal block size in the Mirror Theory would greatly increase the security of one of our constructions. Though, a deeper study of Patarin's theory is required to derive the consequences of this replacement, which is out of the scope of this work.

Leurent et al.'s generic distinguisher on constructions similar to HPxHP with a data complexity of $\mathcal{O}(2^{3n/4})$ queries exploited the occurrence of circles in the underlying hash functions. So, there is still a gap between the best security bound and their attack. We studied that stronger, k-wise independent hash functions decreased the probability of circles where we indicate that it can raise the security level above the bound of $\mathcal{O}(2^{3n/4})$.

We can imagine that the security level of our constructions is higher than $2n/3$ bits. For example, the bottleneck in our proof of HPxNP is the bound for the maximal block size as long as the hash function family is "only" universal. A stronger hash function helps here; plus, it may as well be possible to consider the average block size and obtain $\mathcal{O}(2^n)$ security. However, this needs to be verified.

References

1. Elena Andreeva, Joan Daemen, Bart Mennink, and Gilles Van Assche. Security of Keyed Sponge Constructions Using a Modular Proof Approach. In Gregor Leander, editor, *FSE*, volume 9054 of *LNCS*, pages 364–384. Springer, 2015.
2. Daniel J. Bernstein. Stronger Security Bounds for Wegman-Carter-Shoup Authenticators. In Ronald Cramer, editor, *EUROCRYPT*, volume 3494 of *LNCS*, pages 164–180. Springer, 2005.
3. Daniel J. Bernstein. The Poly1305-AES Message-Authentication Code. In Henri Gilbert and Helena Handschuh, editors, *FSE*, volume 3557 of *LNCS*, pages 32–49. Springer, 2005.
4. Daniel J Bernstein. Polynomial evaluation and message authentication. 2, 2007. `https://cr.yp.to/antiforgery/pema-20071022.pdf`.
5. Larry Carter and Mark N. Wegman. Universal Classes of Hash Functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979.
6. Debrup Chakraborty, Sebati Ghosh, and Palash Sarkar. A Fast Single-Key Two-Level Universal Hash Function. *IACR Trans. Symmetric Cryptol.*, 2017(1):106–128, 2017.
7. Shan Chen and John P. Steinberger. Tight Security Bounds for Key-Alternating Ciphers. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT*, volume 8441 of *LNCS*, pages 327–350. Springer, 2014.
8. Benoît Cogliati, Jooyoung Lee, and Yannick Seurin. New Constructions of MACs from (Tweakable) Block Ciphers. *IACR Trans. Symmetric Cryptol.*, 2017(2):27–58, 2017.
9. Benoît Cogliati and Yannick Seurin. EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO I*, volume 9814 of *LNCS*, pages 121–149. Springer, 2016.
10. Benoît Cogliati and Yannick Seurin. Analysis of the single-permutation encrypted Davies–Meyer construction. *Designs, Codes and Cryptography*, Mar 2018.
11. Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Goutam Paul. Double-block Hash-then-Sum: A Paradigm for Constructing BBB Secure PRF. *IACR Transactions on Symmetric Cryptology*, 2018(3):36–92, Sep. 2018. Full updated version at `https://eprint.iacr.org/2018/804`.
12. Nilanjan Datta, Avijit Dutta, Mridul Nandi, Goutam Paul, and Liting Zhang. Building Single-Key Beyond Birthday Bound Message Authentication Code. Cryptology ePrint Archive, Report 2015/958, 2015. Version: 20160211:123920.
13. Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Kan Yasuda. Encrypt or Decrypt? To Make a Single-Key Beyond Birthday Secure Nonce-Based MAC. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO I*, volume 10991 of *LNCS*, pages 631–661. Springer, 2018.

14. Avijit Dutta, Ashwin Jha, and Mridul Nandi. Exact Security Analysis of Hash-then-Mask Type Probabilistic MAC Constructions. *IACR Cryptology ePrint Archive*, 2016:983, 2016.
15. Avijit Dutta, Ashwin Jha, and Mridul Nandi. Tight Security Analysis of EHtM MAC. *IACR Transactions of Symmetric Cryptology*, 2017(3):130–150, 2017.
16. Avijit Dutta, Mridul Nandi, and Suprita Talnikar. Beyond Birthday Bound Secure MAC in Faulty Nonce Model. *IACR Cryptology ePrint Archive*, 2019:127, 2019. To appear in EUROCRYPT 2019.
17. Shay Gueron and Michael E. Kounavis. Intel Carry-Less Multiplication Instruction and its Usage for Computing the GCM Mode - Rev 2.02. Intel White Paper. Technical report, Intel corporation, April 20 2014.
18. Shay Gueron and Yehuda Lindell. GCM-SIV: Full Nonce Misuse-Resistant Authenticated Encryption at Under One Cycle per Byte. In Indrajit Ray, Ninghui Li, and Christopher Kruegel, editors, *ACM CCS*, pages 109–119. ACM, 2015.
19. Tetsu Iwata and Kazuhiko Minematsu. Stronger Security Variants of GCM-SIV. *IACR Transactions of Symmetric Cryptology*, 2016(1):134–157, 2016.
20. Hugo Krawczyk. LFSR-based Hashing and Authentication. In Yvo Desmedt, editor, *CRYPTO*, volume 839 of *LNCS*, pages 129–139. Springer, 1994.
21. Gaëtan Leurent, Mridul Nandi, and Ferdinand Sibleyras. Generic Attacks Against Beyond-Birthday-Bound MACs. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO I*, volume 10991 of *LNCS*, pages 306–336. Springer, 2018.
22. Atul Luykx and Bart Preneel. Optimal Forgeries Against Polynomial-Based MACs and GCM. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT (1)*, volume 10820 of *LNCS*, pages 445–467. Springer, 2018.
23. Bart Mennink. Towards Tight Security of Cascaded LRW2. In Amos Beimel and Stefan Dziembowski, editors, *TCC II*, volume 11240 of *Lecture Notes in Computer Science*, pages 192–222. Springer, 2018.
24. Bart Mennink and Samuel Neves. Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO III*, volume 10403 of *LNCS*, pages 556–583. Springer, 2017.
25. Kazuhiko Minematsu. How to Thwart Birthday Attacks against MACs via Small Randomness. In Seokhie Hong and Tetsu Iwata, editors, *FSE*, volume 6147 of *LNCS*, pages 230–249. Springer, 2010.
26. Valérie Nachef, Jacques Patarin, and Emmanuel Volte. *Feistel Ciphers - Security Proofs and Cryptanalysis*. Springer, 2017.
27. Mridul Nandi. Birthday Attack on Dual EWCDM. *IACR Cryptology ePrint Archive*, 2017:579, 2017.
28. Mridul Nandi. Bernstein Bound on WCS is Tight - Repairing Luykx-Preneel Optimal Forgeries. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO II*, volume 10992 of *LNCS*, pages 213–238. Springer, 2018.
29. Jacques Patarin. The ”Coefficients H” Technique. In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *SAC*, volume 5381 of *LNCS*, pages 328–345. Springer, 2008.
30. Jacques Patarin. Introduction to Mirror Theory: Analysis of Systems of Linear Equalities and Linear Non Equalities for Cryptography. *IACR Cryptology ePrint Archive*, 2010:287, 2010.
31. Jacques Patarin. Mirror Theory and Cryptography. *IACR Cryptology ePrint Archive*, 2016:702, 2016.
32. Jacques Patarin. Mirror theory and cryptography. *Appl. Algebra Eng. Commun. Comput.*, 28(4):321–338, 2017.

33. Phillip Rogaway. Bucket Hashing and its Application to Fast Message Authentication. In Don Coppersmith, editor, *CRYPTO*, volume 963 of *LNCS*, pages 29–42. Springer, 1995.
34. Victor Shoup. On Fast and Provably Secure Message Authentication Based on Universal Hashing. In Neal Koblitz, editor, *CRYPTO*, volume 1109 of *LNCS*, pages 313–328. Springer, 1996.
35. Mark N. Wegman and Larry Carter. New Classes and Applications of Hash Functions. In *FOCS*, pages 175–182. IEEE Computer Society, 1979.
36. Mark N. Wegman and Larry Carter. New Hash Functions and Their Use in Authentication and Set Equality. *J. Comput. Syst. Sci.*, 22(3):265–279, 1981.
37. Kan Yasuda. A New Variant of PMAC: Beyond the Birthday Bound. In Phillip Rogaway, editor, *CRYPTO*, volume 6841 of *LNCS*, pages 596–609. Springer, 2011.
38. Liting Zhang, Wenling Wu, Han Sui, and Peng Wang. 3kf9: Enhancing 3GPP-MAC beyond the Birthday Bound. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT*, volume 7658 of *LNCS*, pages 296–312. Springer, 2012.

Changelog

2019-01-07: We refined the formulation of Theorem 2 and revised the variables of bad_2 in the analysis of HPxNP.

A Analysis of ξ_{average}

In the following, we show Theorem 4. We restate it to help the reader.

Theorem 6. For any $q \leq 2^n$ and $\varepsilon \leq 1$, we expect that $\xi_{\text{average}} \leq (q-1)\varepsilon + 2$.

Proof Sketch. Note that we argue about an upper bound on the *expected* average block size. To use this argument in a proper security proof, we would also need to bound the amount of collisions such that after q queries no more than q collisions occur. This can be done quite comfortably using Markov's Inequality.

We recall that ξ_{average} is the average block size of non-empty blocks of equations. More formally, we define 2^n bins $i \in \{0, \ldots, 2^n - 1\}$, where each bin i represents the n-bit value i that the hash values $u = h(m)$ can take. Over q queries, we define the number of non-empty bins by $B =^{\text{def}} |\{i : \exists j \in \{1, \ldots, q\} \text{ s.t. } u_j = i\}|$. We denote by ℓ_i the load of the i-th bin, i.e., the number of queries $u = h(m)$ that were equal to i, all over q queries, for $1 \leq i \leq q$. The average bin load over all non-empty bins is given by

$$\ell_{\text{average}} \stackrel{\text{def}}{=} \frac{1}{B} \sum_{i=0}^{2^n-1} \ell_i = \frac{q}{B}$$

since the sum of all bin loads must yield q. We denote by b_i the block size that corresponds to bin i in our proof since a block contains all variables corresponding to tuples (u, ν) with $u = i$ plus the ℓ_i disjoint nonces. So, $b_i =^{\text{def}} \ell_i + 1$ if $\ell_i > 0$ and $b_i =^{\text{def}} 0$ if $\ell_i = 0$, i.e., if bin i is empty. It follows from our definitions above that $\xi_{\text{average}} = \ell_{\text{average}} + 1$. In total, we expect $\binom{q}{2}\varepsilon$ collisions which are distributed over all bins, i.e.,

$$\#\mathsf{Colls} = \binom{q}{2}\varepsilon = \sum_{i=0}^{2^n-1} \binom{\ell_i}{2}. \tag{1}$$

To show the claim, our goal is to maximize ξ_{average}, which is equivalent to maximize ℓ_{average}, which again is equivalent to minimizing B, i.e., the number of non-empty bins.

We have to show two aspects that ℓ_{average} is largest if the distribution of balls is closest possible to uniform while maintaining the expected number of collisions. We can observe that the average block size decreases whenever we would move a ball from one bin to another so that the load of both diverges. Given two disjoint bin indices $i, j \in \{0, \ldots, 2^n - 1\}$ with loads ℓ_i and ℓ_j, respectively. W.l.o.g., we assume that $\ell_i \geq \ell_j$. We have that

$$\#\mathsf{Colls} = \binom{\ell_i}{2} + \binom{\ell_j}{2} + \left(\binom{q}{2}\varepsilon - \binom{\ell_i}{2} - \binom{\ell_j}{2}\right) \overset{\text{def}}{=} \binom{\ell_i}{2} + \binom{\ell_j}{2} + R.$$

We move a ball from bin j to bin i and obtain new loads $\ell'_i = \ell_i + 1$ and $\ell'_j = \ell_j - 1$. We obtain that

$$\#\mathsf{Colls}' = \binom{\ell'_i}{2} + \binom{\ell'_j}{2} + R = \#\mathsf{Colls} + \ell_i - \ell_j + 1 \geq \#\mathsf{Colls} + 2.$$

So, whenever we move a ball such that the resulting bin loads diverge more, the number of collisions used up by those bins increases. Hence, we have less collisions remaining for the remaining bins, which implies that the balls in the remaining bins have to be moved:

- either from some bin i' to j' such that $\ell_{i'} - \ell_{j'} \geq \ell_i - \ell_j$,
- or between multiple bins,
- or balls have to be moved to previously empty bins.

It is easy to see that this configuration is optimal when the individual non-empty bin loads diverge as little as possible. This is given by having B non-empty bins of the same load ℓ_i s. t.

$$\binom{\ell_i}{2} \cdot B = \binom{q}{2}\varepsilon.$$

Since $q = B \cdot \ell_i$, we obtain $\ell_i = (q-1)\varepsilon + 1$. It follows that the maximal average block size is $\xi_{\text{average}} = (q-1)\varepsilon + 2$. □

B Relation to The Attack by Leurent et al.

The attacks in [21] exploit that 4-circles may occur after $2^{3n/4}$ queries if the hash functions are universal, and the messages are constructed in a dedicated manner. We briefly recall the attack by Leurent et al. [21] here.

Attack Description. Leurent et al. considered MACs with $2n$ bits of internal state that can be abstracted to HPxHP. They searched for four-tuples (x, y, z, t) such that they build a 4-circle as:

$$\begin{cases} h_1(x) = h_1(y) \\ h_2(x) = h_2(t) \\ h_1(t) = h_1(z) \\ h_2(y) = h_2(z). \end{cases}$$

Such a tuple can be efficiently verified since it must hold that their corresponding authentication tags sum to zero: $t_x \oplus t_y \oplus t_z \oplus t_t = 0^n$. Since practical instances of such MACs (e.g., PMAC$^+$, 3kf9, Sum-ECBC) hash the message block-wise, they further employ two distinct prefixes p_0 and p_1, such that $|p_0| = |p_1|$ and the prefixes end at the block boundary:

$$x = p_0 \parallel x_*, \quad y = p_1 \parallel y_*, \quad z = p_0 \parallel z_*, \quad t = p_1 \parallel t_*.$$

So, the prefixes lead to differences $\Delta = h_1(p_0) \oplus h_1(p_1)$ and $\nabla = h_2(p_0) \oplus h_2(p_1)$. Considering only four-tuples (x_*, y_*, z_*, t_*) with $x_* \oplus y_* \oplus z_* \oplus t_* = 0^n$, they could translate the problem of finding a solution to the rank-four equation system to the problem of finding a solution to the following rank-three system:

$$\begin{cases} h_1(x) = h_1(y) \\ h_2(x) = h_2(t) \\ h_1(t) = h_1(z) \\ h_2(y) = h_2(z). \end{cases} \quad \Leftrightarrow \begin{cases} h_1(x) = h_1(y) \\ h_2(x) = h_2(t) \\ h_1(t) = h_1(z), \end{cases}$$

with $x_* \oplus y_* = z_* \oplus t_* = \Delta$ and $x_* \oplus t_* = y_* \oplus z_* = \nabla$, From $x_* \oplus y_* \oplus z_* \oplus t_* = 0^n$, it followed then that $h_2(x) = h_2(y)$ also holds. Leurent et al. propose data-efficient algorithms for this 4-sum problem, i.e., finding four-tuples with data complexity of $\mathcal{O}(2^{3n/4})$ queries.

C Analysis of HPxHP with 4-wise-independent Hash Functions

In the following, we show Lemma 7 and 8. We restate both briefly prior to the proofs to help the reader.

Lemma 9. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be independent 4-wise independent hash functions. Let $\xi \geq 7$. Then

$$\Pr\left[\mathsf{bad}_1 | \neg \mathsf{bad}_2\right] \leq \frac{2\binom{q}{4}}{2^{3n}\binom{\xi}{4}} + \frac{16q^5}{2^{4n}}.$$

Proof. The analysis of the maximal block size for HPxHP is a little more delicate than that of HPxNP, because we can have collisions on either side, i.e. in the inputs of π_1 or in the inputs of π_2. We will aim to bound the probability of blocks of size 7 among the queries, i.e., $\{(u_{i_1}, v_{i_1}), \ldots, (u_{i_7}, v_{i_7})\}$, for pairwise distinct $i_1, \ldots, i_7 \in \{1, \ldots, q\}$. For simplicity, we reindex them as $\{(u_1, v_1), \ldots, (u_7, v_7)\}$, hereafter. W.l.o.g., we consider them in an order s. t. $u_i = u_{i+1}$ or $v_i = v_{i+1}$ holds for each $1 \leq i < 7$. We exclude collisions of the form $(u_i, v_i) = (u_j, v_j)$ since those are already covered by bad_2.

For such blocks, we consider sub-blocks of 5 queries (our actual interest) and upper bound their probability. However, not in all cases, we can obtain a satisfying bound; therefore, we will consider 7-blocks at some points. We identify all possible collision patterns and bound their probability accordingly before we can make a final statement on the maximal block size.

The left side of Figure 2 illustrates the possible patterns of 5-chains. We can encode the possible hash-collisions patterns by four-bit strings (a_1, a_2, a_3, a_4), where $a_i = 0$ if $u_i = u_{i+1}$ and $a_i = 1$ if $v_i = v_{i+1}$. It is easy to see that we can obtain at most 16 such patterns indexed from $(0000) = 0$ through $(1111) = 15$. Moreover, the Variants (8) through (15) are symmetric to their counterparts (0) through (7). So, it suffices to bound the probability of the latter. Our claim follows.

Variant (0): $u_1 = u_2 = u_3 = u_4 = u_5$. 4-wise independence unfortunately does not allow a better bound than $q^4/2^{3n}$ for this case. Instead, we allow large collisions in one hash function as long as they are not connected to collisions in the other hash function. This will allow us to bound the probability of large blocks as we did in the analyses before.

For a single hash function, assume that the largest block has size of ξ. This block contains $\binom{\xi}{4}$ 4-collisions. Let $\#\mathsf{4Colls}_1(q)$ denote a random variable for the number of 4-collisions in the outputs of h_1. Again, Markov's Inequality allows us to upper bound the probability that there are more than $\binom{\xi}{4}$ 4-collisions in one hash function by:

$$\Pr\left[\#\mathsf{4Colls}_1(q) \geq \binom{\xi}{4}\right] \leq \frac{\mathbb{E}\left[\#\mathsf{4Colls}_1(q)\right]}{\binom{\xi}{4}} = \frac{\binom{q}{4}}{2^{3n} \cdot \binom{\xi}{4}} \approx \frac{q^4}{2^{3n} \cdot \xi^4}.$$

For $\xi = 2^{n/10}$, this term allows for up to $2^{17n/20}$ queries while the condition $q \cdot \xi^2 = 2^n/67$ is fulfilled for up to $\mathcal{O}(2^{4n/5})$ queries. We can derive a similar argument using a random variable $\#\mathsf{4Colls}_2(q)$ for the number of 4-collisions in the outputs of h_2, So, the probability to obtain a block of size ξ in this case is also approximately at most $2q^4/2^{3n}\xi^4$. In the remainder, we will show that we can upper bound the probability of blocks to a size of $\xi \geq 7$ if they connect collisions in h_1 with collisions in h_2 with a probability of $q^5/2^{4n}$.

Variant (1): $u_1 = u_2 = u_3 = u_4$ and $v_4 = u_5$. From 4-wise independence, it holds that the probability for $u_1 = \ldots = u_4$ is at most

$$\sum_{u_1 \in \{0,1\}^n} \Pr\left[h_1(m_1) = h_1(m_2) = h_1(m_3) = h_1(m_4) = u_1\right] \cdot \Pr\left[v_4 = v_5\right]$$
$$\leq (2^n \cdot 2^{-4n}) \cdot 2^{-n} = 2^{-4n}.$$

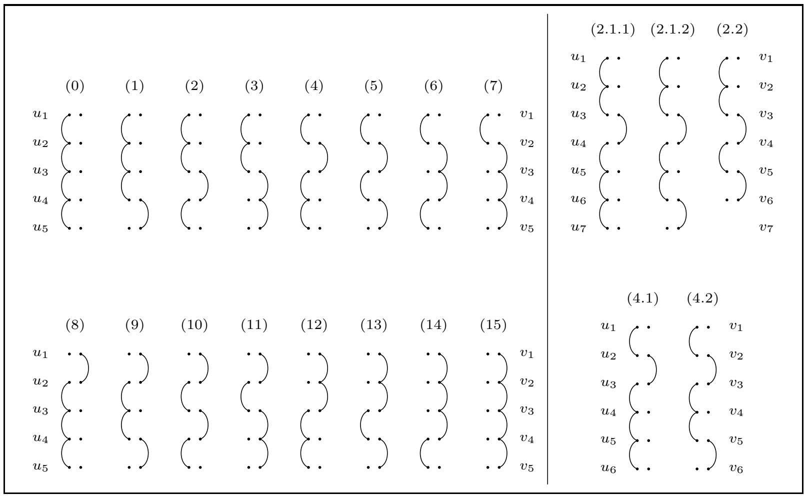


Fig. 2: Structure Graphs of hash-value pairs (u_i, v_i) in blocks of size 5 – 7. Each pair of horizontal dots denotes a pair (u_i, v_i). An edge describes that two hash values are equal, e.g., Variant (2) represents the case that $u_1 = u_2 = u_3$, $v_3 = v_4$, and $u_4 = u_5$.

Since there are at $\binom{q}{5}$ such 5-tuples, this variant has probability at most $q^5/2^{4n}$. An analogous argument can be formulated for Variant (7). For their complexity, we will consider variants (2) and (4) at the end, and proceed with Variant (3) next.

Variant (3): $u_1 = u_2 = u_3$, $v_3 = v_4 = v_5$. From 4-wise independence, it holds

$$\sum_{u_1 \in \{0,1\}^n} \sum_{u_4 \in \{0,1\}^n} \Pr\left[h_1(m_1) = h_1(m_2) = h_1(m_3) = u_1, h_1(m_4) = u_4\right]$$
$$\leq 2^{2n} \cdot 2^{-4n} = 2^{-2n}.$$

Since the outputs of h_2 are independent from h_1, it holds independently

$$\sum_{v_3 \in \{0,1\}^n} \sum_{v_2 \in \{0,1\}^n} \Pr\left[h_2(m_3) = h_2(m_4) = h_2(m_5) = v_3, h_2(m_2) = v_2\right]$$
$$\leq 2^{2n} \cdot 2^{-4n} = 2^{-2n}.$$

We obtain that the upper bound on the probability of this variant is 2^{-4n} for a fixed 5-tuple, and at most $q^5/2^{4n}$ over all such 5-tuples.

Variant (5): $u_1 = u_2$, $v_2 = v_3$, $u_3 = u_4$, $v_4 = v_5$. From our assumption that bad_2 is not set, it holds that $u_1 \neq u_4$ and $v_2 \neq v_5$. Since h_1 and h_2 are independent, it holds that the probability for this constellation is at most

$$\begin{aligned}
&\sum_{u_1 \in \{0,1\}^n} \sum_{u_4 \in \{0,1\}^n} \Pr\left[h_1(m_1) = h_1(m_2) = h_1(m_3) = u_1, h_1(m_4) = u_4\right] \\
&\cdot \sum_{v_2 \in \{0,1\}^n} \sum_{v_4 \in \{0,1\}^n} \Pr\left[h_2(m_2) = h_2(m_3) = v_2, h_2(m_4) = h_2(m_5) = v_4\right] \\
&\leq (2^{2n} \cdot 2^{-4n}) \cdot (2^{2n} \cdot 2^{-4n}),
\end{aligned}$$

and therefore at most $q^5/2^{4n}$ over all 5-tuples.

Variant (6): $u_1 = u_2,\ v_2 = v_3 = v_4,\ u_4 = u_5$. Again, from our assumption that bad_2 is not set, it holds that $u_1 \neq \{u_3, u_4\}$ and $v_2 \notin \{v_1, v_5\}$. Since h_1 and h_2 are independent, it holds that the probability for this constellation is at most

$$\begin{aligned}
&\sum_{v_1 \in \{0,1\}^n} \sum_{v_2 \in \{0,1\}^n} \Pr\left[h_2(m_1) = v_1, h_2(m_2) = h_2(m_3) = h_2(m_3) = v_2\right] \\
&\cdot \sum_{u_1 \in \{0,1\}^n} \sum_{u_4 \in \{0,1\}^n} \Pr\left[h_1(m_1) = h_1(m_2) = u_1, h_1(m_4) = h_1(m_5) = u_4\right] \\
&\leq (2^{2n} \cdot 2^{-4n}) \cdot (2^{2n} \cdot 2^{-4n}),
\end{aligned}$$

and therefore at most $q^5/2^{4n}$ over all 5-tuples.

Variant (2): $u_1 = u_2 = u_3,\ v_3 = v_4,\ u_4 = u_5$. While we could upper bound

$$\Pr\left[u_2 = u_3, v_3 = v_4, u_4 = u_5\right] \leq q^4 \cdot 2^{-3n}$$

in a straight-forward manner for this constellation, it would be inferior to our desired bound. Hence, we extend it further to six-query variants (2.1), where we add the condition $h_1(m_5) = h_1(m_6) = u_5 = u_6$; and (2.2), where we add $h_2(m_5) = h_2(m_6) = v_5 = v_6$. One can observe that constellation (2.2) contains Variant (5). So, the probability for the subset of queries $(m_2, \ldots, m_6)$ to form the collisions as shown can be derived from there to be at most $q^5/2^{4n}$ over all such 5-tuples.

Since we cannot find a good bound for (2.1) yet, we extend it further. We define Variant (2.1.1) to add a seventh query to the block such that $h_1(m_6) = h_1(m_7)$. From 4-wise independence, it holds that the probability for $u_4 = \ldots = u_7$ is at most

$$\begin{aligned}
&\sum_{u_4 \in \{0,1\}^n} \Pr\left[h_1(m_3) = h_1(m_4) = h_1(m_5) = h_1(m_6) = u_4\right] \cdot \Pr\left[v_3 = v_4\right] \\
&\leq (2^n \cdot 2^{-4n}) \cdot 2^{-n} = 2^{-4n}.
\end{aligned}$$

So, the probability for Variant (2.1.1) is at most $q^5/2^{4n}$. For Variant (2.1.2), we can observe that it contains Variant 9, which is axially symmetric to Variant 6.

Thus

$$\sum_{u_3\in\{0,1\}^n}\sum_{u_4\in\{0,1\}^n}\Pr\left[h_1(m_3)=u_3,h_1(m_4)=h_1(m_5)=h_1(m_6)=u_4\right]$$
$$\cdot\sum_{v_3\in\{0,1\}^n}\sum_{v_6\in\{0,1\}^n}\Pr\left[h_2(m_3)=h_2(m_4)=v_3,h_2(m_6)=h_2(m_7)=m_6\right]$$
$$\leq(2^{2n}\cdot 2^{-4n})\cdot(2^{2n}\cdot 2^{-4n})$$

and therefore at most $q^5/2^{4n}$ over all 5-tuples $(m_3,\dots,m_7)$. So, for all extensions, the probability of a 7-query block from Variant (2) is upper bounded by $q^5/2^{4n}$.

Variant (4): $u_1=u_2$, $v_2=v_3$, $u_3=u_4=u_5$. By relabeling the indices of the queries we can see that this variant is the same as Variant (2). □

Lemma 10. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be independent 4-wise independent hash functions. Then

$$\Pr\left[\mathsf{bad}_5|\neg\mathsf{bad}_2\wedge\neg\mathsf{bad}_1\right]\leq\frac{q^4}{2^{4n}}$$

Proof. The analysis of bad_5 can then be conducted as follows, where we restrict our attention to bad_5 conditioned on $\neg\mathsf{bad}_2$ and $\neg\mathsf{bad}_1$. So, we concern chains of even lengths, such that no collisions $(u_i,v_i)=(u_j,v_j)$ has occurred. Hence, bad_2 already covers the probability of 2-chains. A 4-chain is a 4-tuple of pairwise disjoint query indices (i_1,i_2,i_3,i_4) such that there exists an ordering of the indices s. t. $h_1(m_{i_1})=h_1(m_{i_2})$, $h_2(m_{i_2})=h_2(m_{i_3})$, $h_1(m_{i_3})=h_1(m_{i_4})$, and $h_2(m_{i_4})=h_2(m_{i_1})$ hold. For simplicity, we reindex those queries to $(1,2,3,4)$ and reindex their corresponding hash values. It holds that

$$\sum_{u_1\in\{0,1\}^n}\sum_{u_3\in\{0,1\}^n}\Pr\left[h_1(m_1)=h_1(m_2)=u_1,h_1(m_3)=h_1(m_4)=u_3\right]$$
$$\cdot\sum_{v_1\in\{0,1\}^n}\sum_{v_2\in\{0,1\}^n}\Pr\left[h_2(m_1)=h_2(m_4)=v_1,h_2(m_2)=h_2(m_3)=v_2\right]$$
$$\leq(2^{2n}\cdot 2^{-4n})^2=2^{-4n},$$

and over $\binom{q}{4}$ such tuples, we obtain an upper bound of $q^4/2^{4n}$.

A 6-chain is a 6-tuple of pairwise disjoint query indices $(i_1,\dots,i_6)$ such that there exists an ordering of the indices s. t. $h_1(m_{i_1})=h_1(m_{i_2})$, $h_2(m_{i_2})=h_2(m_{i_3})$, $h_1(m_{i_3})=h_1(m_{i_4})$, $h_2(m_{i_4})=h_2(m_{i_5})$, $h_1(m_{i_5})=h_1(m_{i_6})$, and $h_2(m_{i_6})=h_2(m_{i_1})$. Again, we simply reindex them to $(1,\dots,6)$. One can observe that there is a sub-structure that corresponds to Variant (5) in our proof of Lemma 7. By conditioning on $\neg\mathsf{bad}_1$ we do not need to add this term to the above bound. It is easy to see that every chain of eight or more queries must contain at least one of those sub-structures and can be bounded accordingly. Our claim in Lemma 8 follows. □

C.1 Extension to k-independence for Even k

Lemma 11. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be independent k-wise independent hash functions. Then

$$\Pr\left[\mathsf{bad}_1 | \neg\mathsf{bad}_2\right] \leq \frac{2\binom{q}{k}}{2^{(k-1)n} \cdot \binom{\xi}{k}} + \frac{q^{k+1}}{2^{(n-1)k}}.$$

We can extend the argument above to obtain a security of up to $\mathcal{O}(2^{\frac{(n-1)k}{k+1}})$ queries with a k-independent family of hash function. Instead of considering 5-collisions as the base in the proof of Lemma 7, we consider k-collisions in the following. We can index all such $(k+1)$-collision patterns by a k-bit string $(x_1, \ldots, x_k)$ of k variables. Again, each string denotes a collision pattern between a k-tuple of disjoint queries with indices $(i_1, \ldots, i_k)$; So, each bit $x_i = 0$ represents that $h_1(m_i) = h_1(m_{i+1})$ and $x_i = 1$ indicates that $h_2(m_i) = h_2(m_{i+1})$ holds. We denote $h_1(m_i) = u_i$ and $h_2(m_i) = v_i$, for $1 \leq i \leq k$. Again, we exclude cases where $(u_i, v_i) = (u_j, v_j)$ for $i \neq j$.

The probability of almost all collision patterns from such k-bit strings can be easily upper bounded by $q^{k+1}/2^{nk}$. Since we have at most 2^k such patterns, we can upper bound the probability of their union by $2^k q^{k+1}/2^{nk} = q^{k+1}/2^{(n-1)k}$.

The only exceptions are represented by the patterns

- $(010\cdots0), (0010\cdots0), \ldots, (0\cdots010)$,
- and their counterparts $(101\cdots1), (1101\cdots1), \ldots, (1\cdots101)$.

Hence, we will allow these *bad* collision patterns and consider extensions thereof. We focus on those bit strings with hamming weight one since an analog argument holds for their counterparts.

Extending one of those weight-one patterns by a 1-bit on either side will produce a subpattern that has already been excluded. Moreover, we can extend any of the weight-one patterns above to a string of $k-2$ zeros followed by a 1 followed by another $k-2$ zeros. This extended $2(k-1)$-bit string encodes a collision pattern between $2k-1$ queries and is still allowed. However, beyond this point, any further extension will yield an excluded subpattern. Hence, the maximal block size for blocks connecting collisions on the left side with collisions on the right side is $2k$. We define the 0-1-variable $\#\mathsf{kColls}_1(q)$ to be 1 if there exists a chains of k-collisions of hashes from a single hash function, that are not connected to collisions in the second hash functions. Clearly, it can be upper bounded from a similar argument as before for 4-wise independent hash functions:

$$\Pr\left[\#\mathsf{kColls}_1(q) \geq \binom{\xi}{k}\right] \leq \frac{\mathbb{E}\left[\#\mathsf{kColls}_1(q)\right]}{\binom{\xi}{k}} = \frac{\binom{q}{k}}{2^{(k-1)n} \cdot \binom{\xi}{k}} \approx \frac{q^k}{2^{(k-1)n} \cdot \xi^k}.$$

Lemma 12. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be independent k-wise independent hash functions. Then

$$\Pr\left[\mathsf{bad}_5 | \neg\mathsf{bad}_2 \wedge \neg\mathsf{bad}_1\right] \leq \sum_{i=1}^{k/2} \left(\frac{q}{2^n}\right)^{2i}.$$

It remains to exclude circles up to a size of k. Larger circles are excluded by the pattern $(010\dots010)$. Circles up to a size of k can be excluded by $\sum_{i=1}^{k/2}\left(\frac{q}{2^n}\right)^{2i}$.