The Mirror Breaks: Reformulating Cryptographic Proofs for Quantum Realities

Suprita TALNIKAR[1,2] Anandarup ROY[1,3] Kouichi SAKURAI[1]

Abstract: Originating from Patarin's analysis of pseudorandom constructions, Mirror Theory has evolved into a central tool for proving beyond-the-birthday-bound (BBB) security in symmetric-key cryptography. A series of theorems is presented, providing lower bounds on the number of injective solutions under constraints on graph structure and component size (denoted by block maximality, $\xi_{\max}$). Finally, we discuss the potential extension of Mirror Theory from the classical finite domain to the quantum infinite domain.

Keywords: Mirror Theory, BBB Security, Affine equations, Graph Theory

1. Introduction to Mirror Theory in Symmetric Cryptography

On block-size considerations, see AES [1] and PRESENT [2]. For a broad overview of H-coefficients and its applications to PRF/PRP security, see [3], [4]. In symmetric-key cryptography, the security of many constructions is limited by the *birthday bound*. For a cryptographic primitive operating on n-bit blocks, such as a block cipher or permutation, this bound corresponds to a security level of approximately $2^{n/2}$ queries. This limitation arises from the birthday problem in probability theory: after roughly $\sqrt{2^n} = 2^{n/2}$ queries, a collision in the inputs to or outputs from the primitive becomes likely, which can often be exploited by an adversary to distinguish the construction from an ideal one or to forge a message. For many years, this level of security was considered adequate, especially for primitives with large block sizes like the 128-bit AES. An AES-128 based construction with birthday-bound security still offers a formidable 2^{64} security level, which is well beyond the reach of current computational capabilities. However, the cryptographic landscape is evolving. The growing trend towards lightweight cryptography, driven by the proliferation of resource-constrained devices in the Internet of Things (IoT), has led to the standardisation and deployment of block ciphers with smaller block sizes, such as the 64-bit PRESENT. For these ciphers, a birthday-bound security of 2^{32} is insufficient and vulnerable to practical attacks. This necessitates the design of cryptographic modes of operation that offer security guarantees *beyond* the birthday bound (BBB). Achieving BBB security requires more sophisticated design principles and more advanced analytical tools. One of the most powerful and fundamental of these tools is Jacques Patarin's Mirror Theory. It provides a formal mathematical framework for analysing the probability of certain collision events, allowing cryptographers to prove that their constructions remain secure even when the number of queries far exceeds the $2^{n/2}$ threshold.

Historical Origins and Evolution

The origins of Mirror Theory can be traced to the early 2000s and the work of Jacques Patarin, who was investigating the security of classical cryptographic structures. The initial motivation was deeply connected to analysing the security of XOR-of-permutations constructions, a simple yet effective method for building a Pseudorandom Function (PRF) from Pseudorandom Permutations (PRPs) [5], [6], [7]. Schemes such as $XOR_1(x) \coloneqq \pi(0||x) \oplus \pi(1||x)$ and $XOR_2(x) \coloneqq \pi(x) \oplus \pi'(x)$ were of great interest, but proving their security led to a difficult analytical challenge. A security proof required establishing a lower bound on the number of solutions to a system of bivariate affine equations of the form $P_i \oplus P_j = \lambda_{i,j}$, with the critical added constraint that the variables representing permutation outputs must be distinct.

This led Patarin to formulate what he first called the "$P_i \oplus P_j$ Theorem for $\xi_{max} = 2$", which would later be termed Mirror Theory. The parameter ξ_{max} (block maximality) represents the maximum number of variables in the system that become fixed once a single variable is assigned a value; for simple XOR constructions, this value is 2. The theorem, first conjectured in 2003, essentially states that for such a system, the number of distinct solutions is always greater than what one would expect on average for a random

[1] Department of Advanced Informatics, Kyushu University, Fukuoka, Japan
[2] Applied Statistics Unit, Indian Statistical Institute, Kolkata, India
[3] Dr. ROY is supported by the National Institute of Information and Communications Technology(NICT), Japan, under the NICT International Invitational Program.

system.

However, the path to a solid theoretical foundation was fraught with difficulty. Patarin's initial proofs, published across a series of papers and a book, were notoriously complex and opaque. The cryptographic community found them difficult to verify, and it eventually became clear that they contained "unverifiable gaps and several mistakes". This created a precarious and unsettling situation: a powerful and increasingly cited tool, upon which the security claims of numerous constructions rested, was itself built on a foundation that was not fully trusted. This ambiguity was untenable in a field that demands mathematical rigour.

This crisis of verifiability acted as a powerful catalyst, spurring a significant, community-wide research effort to establish a complete and transparently verifiable proof. This endeavour, which included Patarin himself, was ultimately successful, leading to independent, rigorous proofs that solidified the theory's standing and placed it on firm mathematical ground [8], [9], [10], [11]. This journey from a powerful but debated tool to a cornerstone of provable security exemplifies the self-correcting nature of scientific research in a field where absolute certainty is paramount.

The theory's evolution was also driven by the practical needs of cryptographic design. As cryptographers developed more complex and efficient schemes, the analytical requirements grew in tandem. For instance, the security analysis of Message Authentication Codes (MACs) like nEHtM, which involve verification queries that can be rejected, introduced systems containing not just equations but also *non-equations* (e.g., $Y_i \oplus Y_j \neq \lambda'_{ij}$). This practical necessity drove the development of an "Extended Mirror Theory" capable of handling these new types of constraints. Similarly, analysing constructions like the DbHtS MAC in a multi-user setting or the multi-round Feistel cipher generated systems of equations with larger and more complex dependency structures, requiring the generalisation of the theory to arbitrary values of ξ_{max}. This reveals a clear, symbiotic relationship: cryptographic innovation creates new analytical challenges, which in turn drives the evolution of the theoretical tools required to validate them.

1.1 Overview of the Theory and Its Significance

Mirror Theory serves as a counting engine within H-coefficients proofs [12]. Modern, verifiable methods based on link-deletion and recursive inequalities underpin many BBB results [10], [11]. At its core, Mirror Theory is a collection of mathematical theorems that provide a lower bound on the number of pairwise distinct solutions to a system of affine equations and non-equations over a finite group, most commonly $(\{0,1\}^n, \oplus)$. It is not a standalone security proof technique but rather a highly specialised mathematical engine. It is typically employed within a broader proof framework, most notably the H-Coefficients technique, to solve a specific but critical sub-problem: counting the number of valid internal states (e.g., keys, permutation mappings) that could produce a given set of observed inputs and outputs. The significance of Mirror Theory is best understood through its applications. It is the key that unlocks proofs of security far beyond the birthday bound for a wide array of important cryptographic primitives and constructions. The table below provides a roadmap of the constructions that will be analysed in this paper, illustrating the breadth of the theory's impact.

Table 1: Summary of Cryptographic Constructions Analysed with Mirror Theory

Construction	Type	Security	Key Mirror Theory Concepts
XOR of Permutations	PRF from PRP	Optimal ($O(2^n)$) PRF security	Original theorem for $\xi_{max} = 2$; distinctness of solutions.
Feistel Cipher	Block Cipher (PRP)	Optimal ($O(2^n)$) PRP security for ≥ 6 rounds	Generalised theorem for arbitrary ξ_{max}; analysis of complex component structures.
nEHtM	Nonce-Based MAC	BBB security ($\approx 2^{3n/4}$) with graceful degradation	Extended Mirror Theory for non-equations; "Good Graph" conditions (NC, NPL, NCL).
PDMMAC / pEDM	Permutation-Based PRF/MAC	BBB security ($\approx 2^{2n/3}$)	Extended Mirror Theory for $\xi_{max} \leq 3$; analysis of systems with primitive query constraints.
DbHtS	Deterministic MAC	BBB security ($\approx 2^{3n/4}$) in multi-user setting	Refined theory over bipartite graphs; counting solutions in specific algebraic groups.
CLRW2	Tweakable Block Cipher	BBB security ($\approx 2^{3n/4}$)	Analysis of bipartite graphs and complex component partitions.

The paper will begin by delving into the mathematical formalism of Mirror Theory itself, from its graph-theoretic representations to the modern proof techniques based on the link-deletion equation. Finally, it will present detailed case studies of the constructions listed in Table 1, demonstrating precisely how the theory is applied to achieve state-of-the-art security bounds. The necessary background in provable security, focusing on the H-Coefficients technique, is established in the appendix.

2. The Formalism of Mirror Theory

At its core, Mirror Theory addresses a specific combinatorial counting problem, with detailed expositions available in the literature [12], [13], [14]. Consider a system of m affine equations involving p variables, $X_1, \ldots, X_p$, all of which take values in the finite vector space $\{0,1\}^n$. Each equation is *bivariate*, meaning it involves exactly two variables,

and has the general form:

$$X_j \oplus X_k = \lambda_i$$

where $\lambda_i \in \{0,1\}^n$ is a known constant. The fundamental question is to determine how many solution tuples $(X_1, \ldots, X_p) \in (\{0,1\}^n)^p$ exist for this system, subject to the critical constraint that all components of the solution vector must be pairwise distinct (i.e., $X_j \neq X_k$ for all $j \neq k$). Such a solution is referred to as a pairwise distinct (p.d.) or injective solution.

Without the distinctness constraint, this is a standard problem in linear algebra; if the system is consistent, the number of solutions is simply $2^{n(p-m)}$. The distinctness requirement, however, makes the problem significantly harder, as it introduces a large number of implicit non-equations of the form $X_j \oplus X_k \neq 0$, coupling the choices for all variables and making a direct counting approach combinatorially intractable.

2.1 Graph-Theoretic Representation of Affine Systems

To manage this complexity, Mirror Theory employs a graph-theoretic representation that makes the structure of dependencies between variables explicit [12]. A system of equations is mapped to a labelled graph $G = (V, E, L)$, where:

- **Vertices (V):** The set of vertices $V = \{1, \ldots, p\}$ corresponds to the variables $X_1, \ldots, X_p$.
- **Edges (E):** An undirected edge $\{j, k\}$ exists if there is an equation in the system involving variables X_j and X_k.
- **Labels (L):** Each edge $\{j, k\}$ is labelled with the constant λ_i from the corresponding equation $X_j \oplus X_k = \lambda_i$.

This graphical representation transforms an algebraic problem into a structural one. The resulting graph G may consist of one or more connected components. A component is a subgraph in which any two vertices are connected by a path. Assigning a value to any single variable within an acyclic component determines the values of all other variables in that same component. This leads to the definition of a crucial parameter: **block maximality**, denoted ξ_{max}. It is defined as the number of vertices in the largest connected component of the graph G. This parameter quantifies the degree of interdependency among the variables and is a key factor in the bounds provided by Mirror Theory theorems.

For a system to have any pairwise distinct solutions, it must be **p.d.-consistent**. This is a necessary condition ensuring that the equations do not inherently force a collision between variables. This requires that in a "standard form" of the system (where each component is represented as a star graph), all edge labels are non-zero and all labels within a single component are distinct from each other.

2.2 Extended Mirror Theory: Incorporating Non-Equations

Handling non-equations and good-graph conditions is treated in [12]. As noted earlier, the security analysis of many modern cryptographic schemes, particularly MACs, requires considering not only equations but also non-equations of the form $Y_i \oplus Y_j \neq \lambda'_{ij}$. This led to the development of the **Extended Mirror Theory**.

The graph representation is augmented to handle this. The edge set is partitioned into two types: E_{eq} for equations (drawn as solid lines) and E_{neq} for non-equations (drawn as dashed lines). This extension introduces more complex consistency requirements, which are captured by the "good graph" conditions.

2.3 The Good Graph Conditions: NC, NPL, and NCL

For the theorems of Mirror Theory to apply, the graph representing the system must be "good". A good graph is one that is guaranteed to be consistent and non-degenerate. This is ensured by three conditions [15]:

(1) **NC (No Cycle):** The subgraph consisting only of equation edges (E_{eq}) must be acyclic. This prevents linear dependencies and inconsistencies among the equations themselves.

(2) **NPL (Non-Zero Path Label):** For any path P consisting only of equation edges, the XOR-sum of its edge labels, $\mathcal{L}(P)$, must be non-zero. This ensures that no two distinct variables in a component are forced to be equal, which would violate the pairwise distinctness requirement.

(3) **NCL (Non-Zero Cycle Label):** For any cycle C in the full graph that contains *exactly one* non-equation edge, the XOR-sum of all its edge labels, $\mathcal{L}(C)$, must be non-zero. This prevents a situation where the equations along a path force a relationship that directly contradicts the single non-equation in the cycle.

2.4 Formal Statements of Key Theorems

The mathematical core of Mirror Theory consists of several key theorems that provide quantitative bounds for security proofs. The foundational results for the simplest case ($\xi_{\max} = 2$) have been rigorously established [8], [9], while modern techniques have extended these proofs to cover a wide range of parameters [10], [11].

The first theorem addresses the original motivating problem: the security of the XOR of two permutations.

Theorem 1. *Let $\gamma_1, \ldots, \gamma_q$ be any non-zero n-bit strings and $x_1, \ldots, x_q$ be distinct $(n-1)$-bit strings, where $n \geq 12$ and $q \leq 2^n/58$. The probability that a random permutation π over $\{0,1\}^n$ satisfies the system of equations*

$$\pi(x_i||0) \oplus \pi(x_i||1) = \gamma_i \quad \textit{for all } i \in [q]$$

is at least 2^{-nq}.

This theorem provides the foundation for proving the optimal $O(2^n)$ security of constructions like XOR_1. The generalisation of this result to systems with more complex dependency structures is significantly more powerful.

Theorem 2. *Let G be the graph associated with a p.d.-*

consistent system $A_{m\times p}X = \Lambda$ *over* $\{0,1\}^n$. *Let* ξ_{max} *be the size of the largest component of* G. *If* $p \leq \sqrt{N}$ *or* $\sqrt{N} \geq \xi_{max}^2 \log_2 N + \xi_{max}$, *and* $1 \leq p \leq N/(12\xi_{max}^2)$ *(where* $N = 2^n$*), then the number of pairwise distinct solutions to the system is at least:*

$$\frac{(N)_p}{N^m}$$

where $(N)_p = N(N-1)\dots(N-p+1)$ *is the falling factorial.*

This theorem, addressing the foundational case of $\xi_{\max} = 2$, was the subject of the aforementioned historical difficulties. The generalisations of this result to systems with more complex dependency structures are precisely proven, if slightly less powerful.

Finally, the extension of the theory to handle non-equations provides a comprehensive tool for analysing modern cryptographic schemes, such as Message Authentication Codes (MACs).

Theorem 3. *Let* G *be a good graph with* α *vertices,* $|\mathcal{S}| = q_m$ *equation edges, and* $|\mathcal{S}'| = q_v$ *non-equation edges. Let the equation subgraph* $G^{=}$ *have* k *components of sizes* $w_1, \dots, w_k$, *and let* $\sigma_i = \sum_{j=1}^{i} w_j$. *The number of injective solutions chosen from a set of size* $2^n - c$ *is at least:*

$$\frac{(2^n)_\alpha}{2^{nq_m}} \left(1 - \sum_{i=1}^{k} \frac{6\sigma_{i-1}^2 \binom{w_i}{2}}{2^{2n}} - \frac{2(q_v + c\alpha)}{2^n}\right)$$

provided that $\sigma_k w_{max} \leq 2^n/4$.

This extended theorem is the analytical engine behind the security proofs of many state-of-the-art constructions. For example, it is used to establish improved beyond-birthday-bound security for nonce-based MACs like nEHtM [15], and specialised corollaries of it are used to prove tight $O(2^{2n/3})$ security for permutation-based PRFs like PDMMAC [16]. Furthermore, refined versions of the theory tailored to the bipartite graph structures that arise in specific designs have led to tight multi-user security bounds of $O(2^{3n/4})$ for the DbHtS MAC paradigm [17] and similar bounds for tweakable block ciphers like CLRW2 [18], [19]. These applications demonstrate how the formal theorems of Mirror Theory translate directly into the rigorous security guarantees required for modern cryptographic engineering.

Theorem 4. *For systems of equations where the corresponding graph components have a maximum size of three, a specialised corollary of the Extended Mirror Theory applies. This result is crucial for the security analysis of certain permutation-based PRFs, such as PDMMAC, enabling a proof of their tight security bound of* $O(2^{2n/3})$ *queries [16].*

Theorem 5. *For systems of equations whose dependency graph is bipartite, a refined version of Mirror Theory provides a tighter bound on the number of solutions. This result is instrumental in analysing constructions following the Double-block Hash-then-Sum (DbHtS) paradigm* **?**, *establishing a tight multi-user security bound of* $O(2^{3n/4})$ *queries [17].*

Theorem 6. *A highly specialised version of Mirror Theory, which analyses component partitions on a bipartite graph, is used for tweakable block ciphers. This theorem allows for a precise counting of solutions in the analysis of the CLRW2 construction, leading to a tight security bound of approximately* $O(2^{3n/4})$ *queries [18], [19].*

The key result from [8], [9] addresses the original motivating problem: the security of the XOR of two permutations, which corresponds to the case where $\xi_{\max} = 2$.

Theorem 7. *Let* $\gamma_1, \dots, \gamma_q$ *be any non-zero* n*-bit strings and* $x_1, \dots, x_q$ *be distinct* $(n-1)$*-bit strings, where* $n \geq 12$ *and* $q \leq 2^n/58$. *The probability that a random permutation* π *over* $\{0,1\}^n$ *satisfies the system of equations*

$$\pi(x_i||0) \oplus \pi(x_i||1) = \gamma_i \quad \textit{for all } i \in [q]$$

is at least 2^{-nq}.

This theorem provides the foundation for proving the optimal $O(2^n)$ security of constructions like XOR_1. The generalisation of this result to systems with more complex dependency structures, a major contribution from [10], [11] is significantly more powerful.

Theorem 8. *Let* G *be the graph associated with a p.d.-consistent system* $A_{m\times p}X = \Lambda$ *over* $\{0,1\}^n$. *Let* ξ_{max} *be the size of the largest component of* G. *If* $p \leq \sqrt{N}$ *or* $\sqrt{N} \geq \xi_{max}^2 \log_2 N + \xi_{max}$, *and* $1 \leq p \leq N/(12\xi_{max}^2)$ *(where* $N = 2^n$*), then the number of pairwise distinct solutions to the system is at least:*

$$\frac{(N)_p}{N^m}$$

where $(N)_p = N(N-1)\dots(N-p+1)$ *is the falling factorial.*

This generalised theorem is essential for analysing classical structures like the multi-round Feistel cipher, enabling proofs of optimal $O(2^n)$ security by handling the large and intricate component structures that arise from internal collisions [11].

3. Applications in Provable Security: Case Studies

This section demonstrates the practical application of Mirror Theory by analysing the security of several prominent cryptographic constructions. For each case, we describe the construction, show how a security analysis leads to a system of affine equations, and explain how Mirror Theory is applied to derive a beyond-birthday security bound.

3.1 The XOR of Permutations (XORP, $\mathbf{XOR_1}$, $\mathbf{XOR_2}$)

The XOR of permutations is one of the earliest and most fundamental methods for constructing a Pseudorandom Function (PRF) from one or more Pseudorandom Permutations (PRPs). Its security analysis was the original motivation for the development of Mirror Theory, and it serves as the canonical example of the theory's application. The security of this construction has been a subject of intense study, from early analyses by Patarin to later work by

Mennink and Preneel extending the results to the sum of multiple permutations [6], [7].

The two main variants of the construction are:

- **$\mathbf{XOR_2}$ (Two Independent Permutations):** $F_{K_1,K_2}(x) \coloneqq \pi_1(x) \oplus \pi_2(x)$
- **$\mathbf{XOR_1}$ (Single Permutation):** $F_K(x) \coloneqq \pi(0||x) \oplus \pi(1||x)$

Consider the security analysis of XOR_2 in the H-Coefficients framework. An adversary makes q queries with distinct inputs $x_1, \ldots, x_q$ and receives the corresponding outputs $y_1, \ldots, y_q$. In the real world, these outputs are generated by the construction, so for each query $i \in [q]$, the equation $y_i = \pi_1(x_i) \oplus \pi_2(x_i)$ must hold. A transcript $\tau = ((x_1, y_1), \ldots, (x_q, y_q))$ is considered "good" if it contains no trivial flaws. The core of the proof is to find a lower bound for the probability of this transcript occurring, which is proportional to the number of pairs of permutations (π_1, π_2) that are consistent with it.

This consistency requirement can be formulated as a system of equations. Let us define the variables $P_{2i-1} = \pi_1(x_i)$ and $P_{2i} = \pi_2(x_i)$ for $i = 1, \ldots, q$. The transcript imposes the following system of q equations on these $2q$ variables:

$$P_{2i-1} \oplus P_{2i} = y_i, \quad \forall i \in [q]$$

Furthermore, since π_1 and π_2 are permutations and all inputs x_i are distinct, the outputs of each permutation must be distinct. This imposes the pairwise distinctness constraints: the variables $\{P_1, P_3, \ldots, P_{2q-1}\}$ must all be distinct from each other, and the variables $\{P_2, P_4, \ldots, P_{2q}\}$ must also be distinct.

The graph representing this system consists of q disjoint edges, where each edge connects two vertices. Therefore, the block maximality of the system is $\xi_{max} = 2$. This is precisely the scenario addressed by the foundational Mirror Theory theorems, for which Dutta, Nandi, and Saha provided the first complete and verifiable proofs [8], [9]. Applying the theorem for $\xi_{max} = 2$ provides a strong lower bound on the number of valid, injective solutions $(P_1, \ldots, P_{2q})$. This bound on the number of solutions translates directly into a lower bound on the number of permutation pairs (π_1, π_2) that satisfy the transcript. This, in turn, is used to show that the H-Coefficients ratio is very close to 1, ultimately proving that the XORP construction achieves an optimal security bound of $O(2^n)$ queries. This foundational analysis has since been extended with fine-tuned results for more complex scenarios, such as multi-user settings [20].

3.2 Security Analysis of Feistel Ciphers

The Feistel network is a classical and highly influential structure for building block ciphers, most famously used in the Data Encryption Standard (DES). The term often refers to a broad class of generalised Feistel structures, which includes unbalanced and alternating designs [21]. Proving that these ciphers achieve optimal PRP security up to $O(2^n)$ queries for a sufficient number of rounds is a landmark result in symmetric-key cryptography, and one where the generalised form of Mirror Theory is essential.

A k-round Feistel cipher ψ^k operates on an input block split into two halves, (L_0, R_0). Each round j updates the state according to the rule $(L_j, R_j) = (R_{j-1}, L_{j-1} \oplus f_j(R_{j-1}))$, where f_j are the round functions. The security proof involves analysing a transcript of q input/output pairs (P_i, C_i) for the full cipher. The internal state values of the cipher for each query i (e.g., the inputs and outputs of each round function) become the variables in a large system of equations. For example, in a 6-round scheme, we have equations like $X_i = L_i \oplus f_1(R_i)$ and $Y_i = R_i \oplus f_2(X_i)$, where $X_i, Y_i, \ldots$ are internal values.

The analysis becomes significantly more complex than the XORP case because an adversary can choose inputs strategically to induce collisions in these *internal* states. For example, an adversary might submit two different queries, i and j, such that the input to the second round function is the same, i.e., $X_i = X_j$. This internal collision implies a constraint on the first round function: $L_i \oplus f_1(R_i) = L_j \oplus f_1(R_j)$. This equation now links the variables associated with query i to the variables associated with query j. As more such internal collisions occur, a complex dependency graph is built. Unlike the simple graph in the XORP analysis, the graph for a Feistel cipher can have large and intricate connected components. This means that the block maximality, ξ_{max}, can be much greater than 2 and can, in principle, be as large as the number of queries.

This is where the generalised "$P_i \oplus P_j$ Theorem for any ξ_{max}" becomes necessary. The security proof defines "good" transcripts as those where the dependency graph does not contain certain pathological structures (like short cycles, which are handled by the bad transcript analysis). For any such good transcript, the generalised Mirror Theory theorem can be applied. The modern, verifiable proof for this wide-range theorem, along with updated security bounds for Feistel ciphers, was provided by Cogliati et al. [11]. This theorem provides a lower bound on the number of solutions for the round functions $(f_1, \ldots, f_k)$ that are consistent with the transcript, with the bound being parameterised by ξ_{max}. This provides the necessary bound for the H-Coefficients ratio, leading to the celebrated result that a Feistel cipher with six or more rounds is secure as a PRP up to $O(2^n)$ queries. This analytical approach has also been successfully applied to achieve beyond-birthday-bound security for Feistel networks built specifically from random permutations [22].

3.3 Nonce-Based MACs: The Security of nEHtM

nEHtM is a nonce-based Message Authentication Code (MAC) designed to provide beyond-birthday-bound security that degrades gracefully even if the nonce is misused (i.e., repeated). Its security proof is a prime example of the application of the Extended Mirror Theory. The initial analysis by Dutta, Nandi, and Talnikar established its beyond-birthday-bound properties in a faulty nonce model [15], with Choi et al. later providing significantly improved security bounds of approximately $O(2^{3n/4})$ queries [23].

The construction is defined as $nEHtM_{k,k_h}(N, D) \coloneqq E_k(0||N) \oplus E_k(1||(H_{k_h}(D) \oplus N))$, where N is a nonce, D is the data, E_k is a block cipher, and H_{k_h} is a universal hash function. The security game for a MAC involves two types of queries from the adversary:

- **Authentication Queries:** The adversary submits a nonce-data pair (N, D) and receives the correct MAC tag, T.
- **Verification Queries:** The adversary submits a tuple (N', D', T') and asks if T' is a valid tag for (N', D'). A successful forgery occurs if the oracle accepts a tag that was not previously generated by an authentication query.

Let us denote the underlying block cipher (idealised as a permutation π) outputs as $Y_1 = \pi(0||N)$ and $Y_2 = \pi(1||(H_{k_h}(D) \oplus N))$. An authentication query for (N, D) that returns a tag T imposes an **equation** on the system: $Y_1 \oplus Y_2 = T$. A verification query for (N', D', T') that is correctly rejected by the oracle as a forgery imposes a **non-equation**: $Y'_1 \oplus Y'_2 \neq T'$.

The security analysis within the H-Coefficients framework must therefore handle a transcript that generates a mixed system of constraints. The analysis first defines "bad transcripts" to exclude those containing certain collision patterns that would make forgery easy (e.g., multicollisions in nonces or hash values). For a "good transcript," the corresponding graph, which now contains both solid edges for equations and dashed edges for non-equations, must be a "good graph" satisfying the NC, NPL, and NCL conditions described earlier. The Extended Mirror Theory is then applied to this good graph. It provides a lower bound on the number of permutations π that are consistent with the entire transcript of equations and non-equations. This establishes the necessary bound on the H-Coefficients ratio, proving the BBB security of nEHtM and quantifying how that security gracefully degrades as the number of faulty nonces increases.

3.4 Permutation-Based PRFs: PDMMAC and pEDM

A recent trend in symmetric cryptography is the design of schemes based on public permutations, which are often more efficient than traditional block ciphers as they do not require a key schedule. Constructions like PDMMAC by Chakraborti et al. [16] and pEDM by Dutta et al. [24] aim to build BBB-secure Pseudorandom Functions (PRFs) from such public primitives. Their analysis introduces a new layer of complexity that requires a further specialised application of Mirror Theory. The algebraic structures of these constructions are dense, for example:

- **PDMMAC:** $T = \pi^{-1}(\pi(K \oplus M) \oplus 3K \oplus M) \oplus 2K$.
- **pEDM (inverse-free):** $T = \pi(\pi(x \oplus k_1) \oplus (x \oplus k_1) \oplus k_2) \oplus k_1$.

The key difference in the security model is that the adversary can make two types of queries: construction queries to the PRF itself, and *primitive queries* directly to the public permutation π and its inverse π^{-1}. A transcript therefore consists of pairs (M_i, T_i) from the PRF and pairs $(\tilde{u}_j, \tilde{v}_j)$ from the primitive, where $\pi(\tilde{u}_j) = \tilde{v}_j$.

The construction equation for PDMMAC, for instance, can be rewritten as $\pi(T_i \oplus 2K) \oplus \pi(K \oplus M_i) = 3K \oplus M_i$. This induces a system of equations where the variables are the inputs and outputs of the permutation, such as $P_i = K \oplus M_i$ and $Q_i = T_i \oplus 2K$. The primitive queries made by the adversary provide additional, direct information about π, effectively fixing some of these variables or the relationships between them.

The security analysis defines bad transcripts to exclude certain collision patterns that would lead to trivial attacks. For a good transcript, the resulting graph of equations has a bounded component size; specifically, the analysis shows that the components have a size of at most 3. This is a more constrained structure than in the general Feistel case. Therefore, a specialised corollary of the Extended Mirror Theory is used, one which provides a tight bound specifically for systems where components have size 2 or 3. Applying this tailored theorem allows for a precise calculation of the H-Coefficients ratio, leading to a tight security bound of $O(2^{2n/3})$ queries for these constructions. To aid in such analyses, Chen has developed a modular framework that systematises proofs in the ideal-permutation model by extending the ideas of Mirror Theory [25].

3.5 Double-Block Hash-then-Sum (DbHtS) Constructions

The Double-Block Hash-then-Sum (DbHtS) is a general paradigm for building deterministic MACs with beyond-birthday-bound security. The foundational work by Datta et al. unified several existing constructions under this paradigm [26], and Kim et al. later tightened the single-user security bound to $O(2^{3n/4})$ [27]. The multi-user security analysis, which was revisited by Shen et al. [28] and finally made tight by Datta et al. [17], represents a particularly sophisticated application of Mirror Theory.

The DbHtS construction is defined by the paradigm $DbHtS(M) \coloneqq E_{K_1}(\Sigma) \oplus E_{K_2}(\Theta)$, where $(\Sigma, \Theta) = H_{K_h}(M)$ is the output of a double-block length-doubling hash function. In the multi-user setting, an adversary interacts with u users, each with independent keys. A query (i, M_{ia}) to user i with response T_{ia} yields the equation $E_{K_{i1}}(\Sigma_{ia}) \oplus E_{K_{i2}}(\Theta_{ia}) = T_{ia}$.

The security proof involves analysing the complex system of equations generated by many such queries. The key insight in the work of Datta et al. is that this system has a special structure that can be represented as a bipartite graph [17]. One set of vertices represents the Σ hash values and the other represents the Θ values; an edge exists only between a Σ-type vertex and a Θ-type vertex if they are related through an equation. The proof uses a refined version of Mirror Theory specifically for such bipartite graphs to provide a lower bound on the number of solutions for the block cipher outputs. This is used to bound the probability ratio for good transcripts, allowing for the proof of a tight

multi-user security bound of $O(2^{3n/4})$ queries.

3.6 Tweakable Block Ciphers: The Security of CLRW2

The concept of a tweakable block cipher was introduced by Liskov, Rivest, and Wagner as a primitive with three inputs: a key, a message, and a "tweak" [29]. The tweak provides efficient variability without the high cost of changing the cryptographic key. Building on this foundation, Landecker, Shrimpton, and Terashima proposed CLRW2, a construction designed to achieve beyond-birthday-bound (BBB) security by cascading simpler constructions [30]. The security proof of CLRW2 has a notable history, with a flaw in the original proof being identified by Procter [31], and a tight security bound of approximately $O(2^{3n/4})$ queries later being established through the work of Mennink [18] and Jha and Nandi [19].

The CLRW2 construction is a two-round cascade of the LRW2 construction:

$$CLRW2((k_1, k_2, h_1, h_2), t, m) = \\ LRW2((k_2, h_2), t, LRW2((k_1, h_1), t, m)),$$

where $LRW2((k, h), t, m) = E(k, m \oplus h(t)) \oplus h(t)$.

The security proof involves analysing a system of linear equations induced by the construction's algebraic structure. This system is best represented by a bipartite graph, similar to the DbHtS analysis. A highly specialised theorem from Mirror Theory is used, which considers a system of equations induced by a bipartite graph and partitions its components into different types (e.g., isolated vertices, stars centered on different variable types). This detailed structural analysis allows for a very precise counting of the number of valid solutions, which is necessary to achieve the tight security bound.

4. Mirror Theory for Post-Quantum Provable Security

The advent of large-scale quantum computing necessitates a re-evaluation of security for all cryptographic primitives, including the symmetric-key constructions that Mirror Theory is designed to analyse [11], [14]. Unlike asymmetric cryptography, which is often completely broken by Shor's algorithm, symmetric-key schemes are generally considered more resilient. The primary quantum threat is Grover's algorithm [32], which offers a quadratic speed-up on brute-force key searches, effectively halving the security level of a cipher. The standard defence is to double the key size, for instance by moving from AES-128 to AES-256.

This reality does not diminish the importance of beyond-birthday-bound (BBB) security; on the contrary, it heightens it. A construction with a classical security bound of $O(2^n)$ would offer a post-quantum security level of $O(2^{n/2})$ against Grover's algorithm. This is substantially stronger than a birthday-bound construction, whose classical $O(2^{n/2})$ security would degrade to a vulnerable $O(2^{n/4})$ in a post-quantum setting. However, a more subtle and potentially devastating threat comes from structural attacks using algorithms like Simon's, which can exploit algebraic properties in certain constructions to find the key in polynomial time. This means that simply increasing key sizes is not a panacea; the underlying design must also be secure against quantum structural analysis.

The challenge, therefore, is not only to design post-quantum secure symmetric schemes but also to adapt the tools of provable security to a quantum context. This is a profound undertaking, as the entire H-Coefficients framework and its core engine, Mirror Theory, are built on classical foundations. The H-Coefficients technique relies on partitioning a set of classical transcripts, but a quantum adversary can make queries in superposition, fundamentally changing the nature of an interaction. The security proofs must be lifted from the classical Random Oracle Model (ROM) to the Quantum Random Oracle Model (QROM), a notoriously difficult task.

Extending Mirror Theory to this new paradigm is a major open problem. The theory's central function—counting the number of distinct solutions to a system of affine equations derived from a classical transcript—has no obvious quantum analogue. It is not yet clear how to formulate, let alone solve, the equivalent combinatorial problem when an adversary's queries and the resulting transcript exist as a quantum state.

Progress in this area will likely require leveraging the most advanced classical techniques as a starting point. The development of more abstract and modular proof frameworks, which simplify the analysis of complex constructions, is a critical prerequisite for tackling the even greater complexity of quantum proofs [25]. Similarly, the fine-tuned analyses now being applied in complex classical scenarios, such as multi-user settings, demonstrate the level of precision that will be required to reason about the subtle effects of quantum queries [20]. Ultimately, adapting Mirror Theory for a post-quantum world will involve more than just adjusting security bounds; it will demand a reformulation of the fundamental questions of the H-Coefficients technique and a new mathematical language to describe the constraints imposed by a quantum adversary.

Acknowledgments We express our gratitude to the National Institute of Information and Communications Technology (NICT). This research was made possible through the support provided for Dr. Anandarup ROY's visit to Sakurai Lab at Kyushu University by the Foreign Researcher Invitation Program of NICT.

References

[1] National Institute of Standards and Technology. Fips 197: Advanced encryption standard (aes). Technical report, NIST, 2001.

[2] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An ultra-lightweight block cipher. In *Cryptographic Hardware and Embedded Systems – CHES 2007*, volume 4727 of *LNCS*, pages 450–466. Springer, 2007.

[3] Jacques Patarin. The "coefficients h" technique. In *Selected Areas in Cryptography – SAC 2008*, volume 5381 of *LNCS*, pages 328–345. Springer, 2009.
[4] Ashwin Jha and Mridul Nandi. A survey on applications of h-technique: Revisiting security analysis of prp and prf. Technical Report 2018/1130, IACR Cryptology ePrint Archive, 2018.
[5] Jacques Patarin. *Étude des générateurs de permutations pseudo-aléatoires basés sur le schéma du DES*. PhD thesis, Université Pierre et Marie Curie (Paris VI), 1991.
[6] Jacques Patarin. Security in O(2ñ) for the xor of two random permutations – proof with the standard H technique. Technical Report 2013/368, IACR Cryptology ePrint Archive, 2013.
[7] Bart Mennink and Bart Preneel. On the XOR of multiple random permutations. In *Applied Cryptography and Network Security (ACNS 2015)*, pages 619–634. Springer, 2015.
[8] Avijit Dutta, Mridul Nandi, and Abishanka Saha. Proof of mirror theory for $\xi_{\max} = 2$. *IEEE Transactions on Information Theory*, 68(9):6218–6232, 2022.
[9] Avijit Dutta, Mridul Nandi, and Abishanka Saha. Proof of mirror theory for $\xi_{\max} = 2$. Technical Report 2020/669, IACR Cryptology ePrint Archive, 2020.
[10] Benoît Cogliati, Avijit Dutta, Mridul Nandi, Jacques Patarin, and Abishanka Saha. Proof of mirror theory for a wide range of $\xi_{\max}$. Technical Report 2022/686, IACR Cryptology ePrint Archive, 2022.
[11] Benoît Cogliati, Avijit Dutta, Mridul Nandi, Jacques Patarin, and Abishanka Saha. Proof of mirror theory for a wide range of $\xi_{\max}$. In *Advances in Cryptology – EUROCRYPT 2023*, volume 14007 of *Lecture Notes in Computer Science*, pages 470–501. Springer, 2023.
[12] Jacques Patarin. Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography. Technical Report 2010/287, IACR Cryptology ePrint Archive, 2010.
[13] Jacques Patarin. Mirror theory and cryptography. Technical Report 2016/702, IACR Cryptology ePrint Archive, 2016.
[14] Jacques Patarin. Mirror theory and cryptography. *Applicable Algebra in Engineering, Communication and Computing*, 28(3):321–338, 2017.
[15] Avijit Dutta, Mridul Nandi, and Suprita Talnikar. Beyond birthday bound secure MAC in faulty nonce model. Technical Report 2019/127, IACR Cryptology ePrint Archive, 2019.
[16] Avik Chakraborti, Mridul Nandi, Suprita Talnikar, and Kan Yasuda. On the composition of single-keyed tweakable even-mansour for achieving BBB security. *IACR Transactions on Symmetric Cryptology*, 2020(2):1–39, 2020.
[17] Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Suprita Talnikar. Tight multi-user security bound of dbhts. *IACR Transactions on Symmetric Cryptology*, 2023(1):192–223, 2023.
[18] Bart Mennink. Towards tight security of cascaded LRW2. Technical Report 2018/434, IACR Cryptology ePrint Archive, 2018.
[19] Ashwin Jha and Mridul Nandi. Tight security of cascaded LRW2. *Journal of Cryptology*, 33:1272–1317, 2020.
[20] Wonseok Choi, Minki Hhan, Yu Wei, and Vassilis Zikas. On overidealizing ideal worlds: Xor of two permutations and its applications. Technical Report 2023/1704, IACR Cryptology ePrint Archive, 2023.
[21] Viet Tung Hoang and Phillip Rogaway. On generalized feistel networks. Technical report, UC Davis Technical Report, 2010.
[22] Chun Guo and Guoyan Zhang. Beyond-birthday security for permutation-based feistel networks. *Designs, Codes and Cryptography*, 89:407–440, 2021.
[23] Wonseok Choi, Byeonghak Lee, Yeongmin Lee, and Jooyoung Lee. Improved security analysis for nonce-based enhanced hash-then-mask MACs. In *Advances in Cryptology – ASIACRYPT 2020*, volume 12491 of *LNCS*, pages 697–723. Springer, 2020.
[24] Avijit Dutta, Mridul Nandi, and Suprita Talnikar. Permutation based EDM: An inverse free BBB secure PRF. *IACR Transactions on Symmetric Cryptology*, 2021(2):31–70, 2021.
[25] Yu Long Chen. A modular approach to the security analysis of two-permutation constructions. In *Advances in Cryptology – ASIACRYPT 2022*, volume 13791 of *Lecture Notes in Computer Science*, pages 379–409. Springer, 2023.
[26] Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Goutam Paul. Double-block hash-then-sum: A paradigm for constructing BBB secure PRF. Technical Report 2018/804, IACR Cryptology ePrint Archive, 2018.
[27] Seongkwang Kim, Byeonghak Lee, and Jooyoung Lee. Tight security bounds for double-block hash-then-sum MACs. In *Advances in Cryptology – EUROCRYPT 2020*. Springer, 2020.
[28] Yaobin Shen, Lei Wang, Dawu Gu, and Jian Weng. Revisiting the security of DbHtS MACs: Beyond-birthday-bound in the multi-user setting. In *Advances in Cryptology – CRYPTO 2021*, pages 309–336. Springer, 2021.
[29] Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable block ciphers. In *Advances in Cryptology – CRYPTO 2002*, volume 2442 of *LNCS*, pages 31–46. Springer, 2002.
[30] Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable blockciphers with beyond birthday-bound security. In *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *LNCS*, pages 14–30. Springer, 2012.
[31] Gregory J. Procter. A note on the CLRW2 tweakable block cipher construction. Technical Report 2014/111, IACR Cryptology ePrint Archive, 2014.
[32] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, pages 212–219. ACM, 1996.

Appendix

A.1 The H-Coefficients Technique and Provable Security

The H-Coefficients technique is a framework for provable security in which Mirror Theory is applied [3], [4]. It uses a distinguishing game where an adversary attempts to differentiate a real cryptographic construction from an ideal one, like a truly random function. The adversary's success is measured by its advantage.

The method bounds this advantage by partitioning all interaction records, or transcripts, into "good" and "bad" sets [3], [4]. The proof requires showing that bad transcripts are rare in the ideal world (ϵ_{bad}), and that for good transcripts, the real world's probability distribution is close to the ideal world's (ϵ_{ratio}). The advantage is then bounded by $\epsilon_{bad} + \epsilon_{ratio}$.

When analysing $\Pr[X_{re} = \tau]$, we are asking: given a specific transcript τ, what is the probability that a randomly chosen key K and a randomly chosen primitive (e.g., a permutation π) would produce exactly this transcript? This is fundamentally a counting problem. We need to count the number of "valid" keys or internal states that are consistent with the observed transcript τ. The logic of the cryptographic construction imposes a set of mathematical constraints on its internal values. For many constructions based on the XOR operation, these constraints take the form of a system of bivariate affine equations and non-equations. For a good transcript τ, the term $\Pr[X_{re} = \tau]$ is proportional to the number of solutions to this system. This is precisely the problem that Mirror Theory is designed to solve. It provides a robust lower bound on the number of pairwise distinct solutions to such systems. By applying Mirror Theory, we can establish a lower bound on $\Pr[X_{re} = \tau]$, which in turn allows us to prove the second condition of the H-Coefficients technique.