Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory

Bart Mennink[1,2](✉) and Samuel Neves[3]

[1] Digital Security Group, Radboud University, Nijmegen, The Netherlands
b.mennink@cs.ru.nl
[2] CWI, Amsterdam, The Netherlands
[3] CISUC, Department of Informatics Engineering,
University of Coimbra, Coimbra, Portugal
sneves@dei.uc.pt

Abstract. At CRYPTO 2016, Cogliati and Seurin introduced the Encrypted Davies-Meyer construction, $p_2(p_1(x) \oplus x)$ for two n-bit permutations p_1, p_2, and proved security up to $2^{2n/3}$. We present an improved security analysis up to $2^n/(67n)$. Additionally, we introduce the dual of the Encrypted Davies-Meyer construction, $p_2(p_1(x)) \oplus p_1(x)$, and prove even tighter security for this construction: $2^n/67$. We finally demonstrate that the analysis neatly generalizes to prove almost optimal security of the Encrypted Wegman-Carter with Davies-Meyer MAC construction. Central to our analysis is a modernization of Patarin's mirror theorem and an exposition of how it relates to fundamental cryptographic problems.

Keywords: PRP-to-PRF · Encrypted Davies-Meyer · Encrypted Davies-Meyer dual · EWCDM · Optimal security

1 Introduction

Many cryptographic primitives rest on the assumption that their building blocks behave as perfectly random functions. This is the case for, among many others, encryption modes [4], authenticators [5,9], or random permutations [28]. Yet, for all their utility, very few pseudorandom functions are actually available to practitioners. Instead, the leading cryptographic building block is the pseudorandom permutation, also known as the block cipher. It is therefore common practice to employ block ciphers as stand-ins for pseudorandom functions.

To a first approximation, this solves the problem. The PRP-PRF switch [6,8,13,21,24] tells us that a PRF can be safely replaced by a PRP up to approximately $2^{n/2}$ queries. With large blocks this is often acceptable, but for lightweight block ciphers, whose number has grown tremendously in recent years (e.g., [1,2,11,12,18,20,22,27,46,51]), this $2^{n/2}$ birthday bound severely limits the application range. For example, Bhargavan and Leurent [10] recently presented practical collision attacks on TLS if a 64-bit cipher is used.

J. Katz and H. Shacham (Eds.): CRYPTO 2017, Part III, LNCS 10403, pp. 556–583, 2017.
DOI: 10.1007/978-3-319-63697-9_19

In order to save these ciphers from obsolescence, various PRP-to-PRF constructions have been presented that achieve security beyond the $2^{n/2}$ security bound. We can categorize these into truncation-based solutions and xor-based solutions.[1] Here and throughout, we simply talk about permutations to refer to block ciphers instantiated with a secret key, unless explicitly stated otherwise.

Truncation. Hall et al. [21] suggested simple truncation. Bellare and Impagliazzo [3] and Gilboa and Gueron [19] proved that truncating an n-bit permutation by $m < n$ bits has security up to approximately $2^{\frac{m+n}{2}}$ queries. This result was, as a matter of fact, already derived around 20 years earlier by Stam [47], be it in a non-cryptographic context.

Xor of Permutations. The xor (or more generally, sum) of two permutations,

$$\mathrm{XoP}^{p_1,p_2}(x) = p_1(x) \oplus p_2(x)\,, \tag{1}$$

where p_1, p_2 are two permutations, was initially mentioned by Bellare et al. [7] as a "natural" PRP-to-PRF method, and was later analyzed by Lucks [29] and Bellare and Impagliazzo [3]. Patarin achieved $2^n/67$ security [39,40,42]. The results are natively inherited by the construction that consists of the xor of three or more independent permutations [16,30].

The xor of permutations evidently requires independence between p_1 and p_2. If only a single permutation is to be used, one can simulate this independence through domain separation, as suggested by Lucks [29] and Bellare and Impagliazzo [3]:

$$\mathrm{XoP}'^{p}(x) = p(0\|x) \oplus p(1\|x)\,. \tag{2}$$

Patarin [40] proved that this single permutation construction achieves a similar level of security as XoP.

A New Contender. At CRYPTO 2016, Cogliati and Seurin [17] introduced the Encrypted Davies-Meyer (EDM) construction (see Fig. 1a):

$$\mathrm{EDM}^{p_1,p_2}(x) = p_2(p_1(x) \oplus x)\,, \tag{3}$$

where p_1, p_2 are two permutations. Cogliati and Seurin proved that EDM^{p_1,p_2} behaves like a random function up to complexity $2^{2n/3}$, and actually conjectured that 2^n is possible.

EDM^{p_1,p_2} shows structural differences with the xor of permutations, and these differences allowed Cogliati and Seurin to devise the misuse-resistant MAC

[1] Another notable approach is data-dependent rekeying by Bellare et al. [7]: given a block cipher E_k, data-dependent rekeying computes $E_{E_k(x)}(x)$. However, this approach only achieves approximately $2^{n/2}$ security, and it inherently requires rekeying of the block cipher which could be a costly operation in practice.

function Encrypted Wegman-Carter with Davies-Meyer (EWCDM), defined as follows:

$$\mathrm{EWCDM}^{h,p_1,p_2}(\nu, m) = p_2(p_1(\nu) \oplus \nu \oplus h(m))\,, \tag{4}$$

where h is an almost xor universal hash function, p_1, p_2 are two permutations, and where ν denotes the nonce and m the message, which may be arbitrarily large. Cogliati and Seurin proved that $\mathrm{EWCDM}^{h,p_1,p_2}$ achieves security up to $2^{2n/3}$ in the nonce-respecting setting, and $2^{n/2}$ security in the nonce-misusing setting. They likewise conjectured optimal 2^n security in the nonce-respecting setting.

1.1 Our Contribution

We improve the security of EDM^{p_1,p_2} as well as $\mathrm{EWCDM}^{h,p_1,p_2}$ from $2^{2n/3}$, as derived by Cogliati and Seurin [17], to $2^n/(67n)$. Furthermore, we introduce the dual of EDM, the Encrypted Davies-Meyer Dual (EDMD) construction:

$$\mathrm{EDMD}^{p_1,p_2}(x) = p_2(p_1(x)) \oplus p_1(x)\,. \tag{5}$$

The dual is depicted in Fig. 1b, and as can be seen from a simple comparison with EDM^{p_1,p_2} of Fig. 1a, the constructions are very much related, and equally expensive. We show that the EDMD construction achieves security up to $2^n/67$ queries.

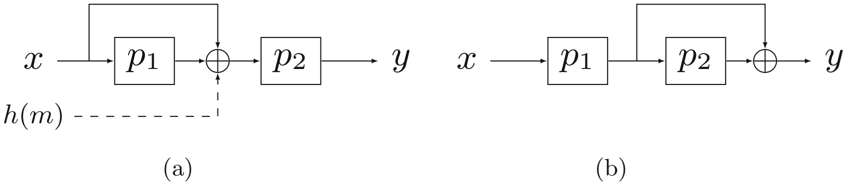

Fig. 1. Encrypted Davies-Meyer (a) and its dual (b). The dashed line represents the necessary addition to yield EWCDM.

Mirror Theory. The backbone of our security analysis is Patarin's mirror theory [31,36,40,43], a very powerful but rather unknown technique. We refurbish and modernize it in Sect. 3 in order to be able to neatly apply it in our analyses.

At a basic level, the idea of Patarin's mirror theory is to consider $q \geq 1$ equations in $r \geq q$ unknowns, and to determine a lower bound on the number of possible solutions to the unknowns. Some conditions naturally apply: the q equations are of the form $P_a \oplus P_b = \lambda$,[2] where P_a and P_b are two unknowns, and the solution to the unknowns should not contain collisions.

[2] Generalizations to multiple unknowns are possible [40,43], but are irrelevant for our work.

Consider the following example system of equations:

$$P_a \oplus P_b = \lambda_1 \, , \; P_b \oplus P_c = \lambda_2 \, , \; P_d \oplus P_e = \lambda_3 \, . \tag{6}$$

We have 2^n choices for P_a, after which P_b is determined by λ_1 and P_c by λ_2. Next, we have $2^n - 3$ options for P_d (as P_d should not collide with P_a, P_b, and P_c), after which P_e is determined by λ_3. This naive counting gives $2^n(2^n - 3)$ solutions to the system of equations, but it disregards two potential problems: (i) the choice may result in a collision in the unknowns and (ii) the system of equations may be inconsistent in the first place. Problem (i) may occur in a straightforward way if, for instance, $\lambda_1 = 0$, as in this case the first equation states that $P_a = P_b$. It could also happen in a more delicate setting, for example if $P_b = P_e$ (even though P_d does not collide with P_a). To understand problem (ii), consider the system of equations of (6) *appended with* equation $P_a \oplus P_c = \lambda_4$. From the first two equations of (6) and the appended equation we can conclude that the system is inconsistent if $\lambda_1 \oplus \lambda_2 \oplus \lambda_4 \neq 0$.

If problem (i) or (ii) occurs, the system of equations naturally has no solution. Disregarding these two problems, the fundamental mirror theorem states that if the number of q equations is “small enough,” then the number of solutions to the r unknowns is at least $\frac{(2^n)_r}{2^{nq}}$, where $(2^n)_r$ is the falling factorial. What it means for q to be “small enough” depends on the system of equations under investigation. We refer to Theorem 2 for the details. We will in fact use a generalization of this theorem, where the solution to the unknowns may contain some collisions (see Theorem 3).

The bound itself is merely a combinatorial lower bound whose relevance is not that clear at first sight. Its strength lies in the fact that it can be nicely employed within the H-coefficient technique by Patarin [15,33,37], and in particular, it forms a crucial part in proving the (almost) optimal security of EDM, EWCDM, and EDMD.

Patarin's mirror theorem (or variants thereof) has been used already to analyze the security of Feistel constructions and the xor of permutations by Patarin [34–36,38–42,45], Cogliati et al. [16], and Volte et al. [48,49]. Iwata et al. [26] recently pointed out that a result from Patarin's mirror theorem implies almost optimal security of CENC [25].

Security of EDM. By looking at EDM^{p_1,p_2} from a different angle, we can prove $2^n/(67n)$ security for the case of independent permutations p_1, p_2 (Sect. 4). In more detail, we regard EDM^{p_1,p_2} as a sum of permutations *in the middle*, where an evaluation $y = \mathrm{EDM}^{p_1,p_2}(x)$ corresponds to a xor of permutations as $p_1(x) \oplus p_2^{-1}(y) = x$. After this we only need to overcome a few technicalities in order to apply the mirror theorem.

Security of EWCDM. Our analysis of EDM^{p_1,p_2}, namely the restructuring of the data flows, generalizes to $\mathrm{EWCDM}^{h,p_1,p_2}$ *almost verbatim*. In more detail, we prove in Sect. 5 that, in the nonce-respecting setting, $\mathrm{EWCDM}^{h,p_1,p_2}$ achieves close to optimal $2^n/(67n)$ PRF security. The analysis straightforwardly generalizes to MAC security. Security in the nonce-misusing setting cannot exceed the birthday bound as derived in [17].

Security of EDMD. Similar techniques allow us to prove optimal security of EDMD based on independent permutations. However, in Sect. 6 we observe that its security reduces quite elegantly to the xor of two independent permutations, XoP^{p_1,p_2} of (1). Therefore, EDMD based on independent permutations achieves $2^n/67$ security.

Towards a Single Permutation. Our results on EDM^{p_1,p_2} and $\mathrm{EWCDM}^{h,p_1,p_2}$ satisfactorily resolve the conjecture put forward by Cogliati and Seurin [17] up to a logarithmic factor, and our construction EDMD^{p_1,p_2} even achieves better security than EDM^{p_1,p_2}. Cogliati and Seurin furthermore conjectured that optimal security is already achieved *in the identical permutation case*, i.e., where $p_1 = p_2$. We support this conjecture, and think that it also holds for the dual, but it appears unlikely that the techniques used in this work can be employed to prove optimal security of EDM^p or EDMD^p, let alone $\mathrm{EWCDM}^{h,p}$. In Sect. 7 we give informal justification for this claim, and discuss further possibilities to investigate EDM^p and EDMD^p.

A Dual of EWCDM? An earlier version of this article suggested, as a side result, the dual construction

$$\mathrm{EWCDMD}^{h,p_1,p_2}(\nu, m) = p_2(p_1(\nu) \oplus h(m)) \oplus p_1(\nu) \oplus h(m)\,, \tag{7}$$

with a claimed security of $2^n/(67n)$. However, Nandi [32] pointed out that $\mathrm{EWCDMD}^{h,p_1,p_2}$ can be seen as a cascade of two non-injective functions, therewith having twice as many collisions as expected, and can be distinguished from random in about $2^{n/2}$ queries. Closer inspection of the security proof revealed a very subtle issue in the application of the mirror theory, namely that it cannot readily handle systems of equations with a *conditional* existence of (in-)equalities, e.g., where two unknowns must be equal if two other unknowns satisfy a certain condition.[3] Broadly speaking, the problem is similar to (but more subtle than) issues encountered when analyzing a single permutation variant EDM^p, EDMD^p, or $\mathrm{EWCDM}^{h,p}$ (cf. Sect. 7). As such, we consider it to be a non-trivial exercise to derive a dual of $\mathrm{EWCDM}^{h,p}$ that provably achieves security beyond the birthday bound. We remark that $\mathrm{EWCDMD}^{h,p_1,p_2}$ may still achieve MAC security beyond the birthday bound, however, we have not considered MAC security in this work as it is beyond the scope of the article.

[3] The issue does not appear for EDM^{p_1,p_2} or $\mathrm{EWCDM}^{h,p_1,p_2}$. It even does not appear for EDMD^{p_1,p_2} as the inputs to the second permutation are always distinct.

2 Preliminaries

For a natural number n, $\{0,1\}^n$ denotes the set of all n-bit strings, and we denote by $\{0,1\}^*$ the set of bit strings of arbitrary length. $\mathsf{func}(n)$ denotes the set of all functions on $\{0,1\}^n$, and $\mathsf{perm}(n)$ the set of all permutations. We denote by $\mathsf{func}(n+*,n)$ the set of all functions with domain $\{0,1\}^n \times \{0,1\}^*$ and range $\{0,1\}^n$. For a natural number $m \geq n$, we write $(m)_n = m(m-1)\cdots(m-n+1)$ as the falling factorial. For a set $\mathcal{X}$, $x \xleftarrow{\$} \mathcal{X}$ denotes uniformly random sampling of x from $\mathcal{X}$.

2.1 Universal Hash Functions

For two non-empty sets $\mathcal{X}, \mathcal{Y}$, a family of hash functions $H = \{h : \mathcal{X} \to \mathcal{Y}\}$ is said to be ϵ-AXU (almost xor universal) if for any distinct $x, x' \in \mathcal{X}$ and $y \in \mathcal{Y}$, we have

$$\mathbf{Pr}\left[h \xleftarrow{\$} H \;:\; h(x) \oplus h(x') = y\right] \leq \epsilon \,.$$

2.2 Distinguishers

A distinguisher $\mathcal{D}$ is a computationally unbounded adversary that is given adaptive access to an oracle $\mathcal{O}$ and outputs a bit 0/1. For two oracles $\mathcal{O}$ and $\mathcal{P}$ with identical interface, we denote the distinguishing advantage of $\mathcal{D}$ by

$$\varDelta_{\mathcal{D}}(\mathcal{O}\,;\,\mathcal{P}) = \mathbf{Pr}\left[\mathcal{D}^{\mathcal{O}} \Rightarrow 1\right] - \mathbf{Pr}\left[\mathcal{D}^{\mathcal{P}} \Rightarrow 1\right] \,. \tag{8}$$

Throughout this work, we only consider computationally unbounded distinguishers whose complexities are solely measured by the number of queries to the oracle. Without loss of generality, it suffices to only focus on deterministic distinguishers, as for any probabilistic distinguisher there exists a deterministic one with at least the same success probability, and we will assume so henceforth.

2.3 H-Coefficient Technique

Central to our analysis will be the H-coefficient technique by Patarin [33,37], and as a matter of fact, the mirror theory of Sect. 3 will be a useful tool *within* this technique. We will follow the renewed description of Chen and Steinberger [15].

Consider two oracles $\mathcal{O}$ and $\mathcal{P}$, and an information-theoretic deterministic distinguisher $\mathcal{D}$ with query complexity q that tries to distinguish both oracles: $\varDelta_{\mathcal{D}}(\mathcal{O}\,;\,\mathcal{P})$ of (8). The communication that $\mathcal{D}$ has with its oracle is recorded in a transcript τ. Denote by $X_{\mathcal{O}}$ the probability distribution of transcripts when $\mathcal{D}$ is interacting with $\mathcal{O}$, and similarly by $X_{\mathcal{P}}$ the distribution of transcripts for interaction with $\mathcal{P}$. Say that a transcript is "attainable" if $\mathbf{Pr}\left[X_{\mathcal{P}} = \tau\right] > 0$ and denote by $\mathcal{T}$ the set of all attainable transcripts.

The H-coefficient technique states the following:

Theorem 1 (H-coefficient technique). *Let $\delta, \varepsilon \in [0,1]$. Consider a partition $\mathcal{T} = \mathcal{T}_{\text{bad}} \cup \mathcal{T}_{\text{good}}$ of the set of attainable transcripts such that*

1. $\mathbf{Pr}\left[X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}}\right] \leq \delta$,
2. *for all* $\tau \in \mathcal{T}_{\text{good}}$, $\dfrac{\mathbf{Pr}\left[X_{\mathcal{O}} = \tau\right]}{\mathbf{Pr}\left[X_{\mathcal{P}} = \tau\right]} \geq 1 - \varepsilon$.

Then, the distinguishing advantage satisfies $\Delta_{\mathcal{D}}(\mathcal{O}\,;\,\mathcal{P}) \leq \delta + \varepsilon$.

Proof. A proof of the technique is given among others in [14,15], and we repeat it briefly. As we consider a deterministic distinguisher $\mathcal{D}$, its advantage is equal to the statistical distance between the distributions of views $X_{\mathcal{O}}$ and $X_{\mathcal{P}}$:

$$\begin{aligned}
\Delta_{\mathcal{D}}(\mathcal{O}\,;\,\mathcal{P}) &= \frac{1}{2}\sum_{\tau\in\mathcal{T}} \left|\mathbf{Pr}\left[X_{\mathcal{O}} = \tau\right] - \mathbf{Pr}\left[X_{\mathcal{P}} = \tau\right]\right| \\
&= \sum_{\tau\in\mathcal{T}:\mathbf{Pr}[X_{\mathcal{P}}=\tau]>\mathbf{Pr}[X_{\mathcal{O}}=\tau]} \left(\mathbf{Pr}\left[X_{\mathcal{P}} = \tau\right] - \mathbf{Pr}\left[X_{\mathcal{O}} = \tau\right]\right) \\
&= \sum_{\tau\in\mathcal{T}:\mathbf{Pr}[X_{\mathcal{P}}=\tau]>\mathbf{Pr}[X_{\mathcal{O}}=\tau]} \mathbf{Pr}\left[X_{\mathcal{P}} = \tau\right]\left(1 - \frac{\mathbf{Pr}\left[X_{\mathcal{O}} = \tau\right]}{\mathbf{Pr}\left[X_{\mathcal{P}} = \tau\right]}\right).
\end{aligned}$$

Making a distinction between bad and good views, we find:

$$\Delta_{\mathcal{D}}(\mathcal{O}\,;\,\mathcal{P}) \leq \sum_{\tau\in\mathcal{T}_{\text{bad}}} \mathbf{Pr}\left[X_{\mathcal{P}} = \tau\right] + \sum_{\tau\in\mathcal{T}_{\text{good}}} \mathbf{Pr}\left[X_{\mathcal{P}} = \tau\right]\varepsilon \leq \delta + \varepsilon\,,$$

which completes the proof. □

The basic idea of the technique is that a large number of transcripts are almost equally likely in both worlds, and the odd ones appear only with negligible probability δ. Note that the partitioning of $\mathcal{T}$ into bad and good transcripts is directly reflected in the terms δ and ε in the bound: if $\mathcal{T}_{\text{good}}$ is too large, ε will become large, whereas if $\mathcal{T}_{\text{bad}}$ is too large, δ will become large.

For a given transcript $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$ consisting of q input/output tuples, we say that an oracle $\mathcal{O}$ *extends* τ, denoted $\mathcal{O} \vdash \tau$, if

$$\mathcal{O}(x_i) = y_i$$

for $i = 1, \ldots, q$.

2.4 Pseudorandom Function Security

Let $F^{p_1,p_2} \in \mathsf{func}(n)$ be a fixed-input-length function that internally uses two permutations $p_1, p_2 \in \mathsf{perm}(n)$. We denote the PRF security of F as a random function by

$$\mathbf{Adv}^{\text{prf}}_{F^{p_1,p_2}}(\mathcal{D}) = \Delta_{\mathcal{D}}(F^{p_1,p_2}\,;\,f) \tag{9}$$

where the probabilities are taken over the drawing of $p_1, p_2 \xleftarrow{\$} \mathsf{perm}(n)$ and $f \xleftarrow{\$} \mathsf{func}(n)$.

The model generalizes to the security of variable-input-length functions as follows. Let $F^{h,p_1,p_2} \in \mathsf{func}(n+*, n)$ be a variable-input-length function that internally uses two permutations $p_1, p_2 \in \mathsf{perm}(n)$ and a universal hash function h from some hash function family H. We denote the PRF security of F as a random function by

$$\mathbf{Adv}^{\mathrm{prf}}_{F^{h,p_1,p_2}}(\mathcal{D}) = \Delta_{\mathcal{D}}(F^{h,p_1,p_2}\,;\, f) \tag{10}$$

where the probabilities are taken over the drawing of $h \xleftarrow{\$} H$, $p_1, p_2 \xleftarrow{\$} \mathsf{perm}(n)$, and $f \xleftarrow{\$} \mathsf{func}(n+*, n)$. For variable-input-length functions, we will impose that $\mathcal{D}$ is nonce-respecting, i.e., it never makes two queries to its oracle with the same first component.

Remark 1. We focus on PRF security in the information-theoretic setting, where the underlying primitives are secret permutations uniformly randomly drawn from $\mathsf{perm}(n)$. Our results straightforwardly generalize to the complexity-theoretic setting, where the permutations are instantiated as E_{k_1}, E_{k_2} for secret keys k_1, k_2. The bounds of this work carry over with an additional loss of $2\mathbf{Adv}^{\mathrm{prp}}_{E}(q)$, where $\mathbf{Adv}^{\mathrm{prp}}_{E}(q)$ denotes the maximum advantage of distinguishing E_k for secret k from a uniformly random permutation in q queries. Note that in our analyses, the distinguisher can *only* induce forward evaluations of the underlying primitive. Therefore, the block cipher only needs to be prp secure, and not necessarily sprp secure.

3 Mirror Theory

We revisit an important result from Patarin's mirror theory [36,40] in our context of pseudorandom function security. For the sake of presentation and interoperability with the results in the remainder of this paper, we use different parametrization and naming of definitions.

3.1 System of Equations

Let $q \geq 1$ and $r \geq 1$. Let $\mathcal{P} = \{P_1, \ldots, P_r\}$ be r unknowns, and consider a system of q equations

$$\mathcal{E} = \{P_{a_1} \oplus P_{b_1} = \lambda_1, \cdots, P_{a_q} \oplus P_{b_q} = \lambda_q\} \tag{11}$$

where a_i, b_i for $i = 1, \ldots, q$ are mapped to $\{1, \ldots, r\}$ using some surjective index mapping

$$\varphi : \{a_1, b_1, \ldots, a_q, b_q\} \to \{1, \ldots, r\}\,.$$

Note that for a given system of equations, the index mapping is unique up to a reordering of the unknowns. There is a one-to-one correspondence between $\mathcal{E}$ on the one hand and $(\varphi, \lambda_1, \dots, \lambda_q)$ on the other hand, and below definitions are mostly formalized based on the latter description (but it is convenient to think about them with respect to $\mathcal{E}$). For a subset $I \subseteq \{1, \dots, q\}$ we define by $\mathcal{M}_I$ the multiset

$$\mathcal{M}_I = \bigcup_{i \in I} \{\varphi(a_i), \varphi(b_i)\}\,.$$

We give three definitions with respect to the system of equations $\mathcal{E}$.

Definition 1 (circle-freeness). *The system of equations $\mathcal{E}$ is* circle-free *if there is no $I \subseteq \{1, \dots, q\}$ such that the multiset $\mathcal{M}_I$ has even multiplicity elements only.*

Definition 2 (block-maximality). *Let $\{1, \dots, r\} = \mathcal{R}_1 \cup \cdots \cup \mathcal{R}_s$ be a partition of the r indices into s minimal "blocks" such that for all $i \in \{1, \dots, q\}$ there exists an $\ell \in \{1, \dots, s\}$ such that $\{\varphi(a_i), \varphi(b_i)\} \subseteq \mathcal{R}_\ell$. The system of equations $\mathcal{E}$ is* ξ-block-maximal *for $\xi \geq 2$ if there is no $\ell \in \{1, \dots, s\}$ such that $|\mathcal{R}_\ell| > \xi$.*

Definition 3 (non-degeneracy). *The system of equations $\mathcal{E}$ is* non-degenerate *if there is no $I \subseteq \{1, \dots, q\}$ such that the multiset $\mathcal{M}_I$ has exactly two odd multiplicity elements and such that $\bigoplus_{i \in I} \lambda_i = 0$.*

Informally, circle-freeness means that there is no linear combination of one or more equations in $\mathcal{E}$ that is independent of the unknowns, block-maximality means that the unknowns can be partitioned into blocks of a certain maximum size such that there is no linear combination of two or more equations in $\mathcal{E}$ that relates two unknowns P_a, P_b from different blocks $\mathcal{R}_i, \mathcal{R}_j$, and non-degeneracy means that there is no linear combination of one or more equations that implies $P_a = P_b$ for some $P_a, P_b \in \mathcal{P}$.

3.2 Main Result

The main theorem of Patarin's mirror theory, simply dubbed "mirror theorem", is the following. It corresponds to "Theorem $P_i \oplus P_j$ for any ξ_{max}" of Patarin [40, Theorem 6].

Theorem 2 (mirror theorem). *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 for $\mathcal{P}$ such that $P_a \neq P_b$ for all distinct $a, b \in \{1, \dots, r\}$ is at least*

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

The quantity measured in above theorem (the number of solutions...) is called h_r in [40]. H_r is subsequently defined as $2^{nq} h_r$. The parameter H has slightly different meanings in [39,41,42], namely the number of oracles whose outputs could solve the system of equations. In the end, these definitions yielded the naming of the H-coefficient technique of Theorem 1. For the mirror theorem, we have opted to stick to the convention of [40] as its definition is pure in the sense that it is independent of the actual oracles in use.

In Appendix A, we give a proof sketch of Theorem 2, referring to [40] for the details. In the proof sketch, it becomes apparent that the side condition $(\xi-1)^2 \cdot r \leq 2^n/67$ can be improved (even up to $2^n/16$) quite easily. Patarin first derived the side condition symbolically and only then derived the specific constants. Knowing the constants in advance, we reverted the reasoning. However, to remain consistent with the theorem statement of [40], we deliberately opted to leave the 67 in; the improvement is nevertheless only constant. The term $(\xi-1)^2$ is present to cover worst-case systems of equations; it can be improved to $(\xi-1)$ in certain cases [44]. Fortunately, in most cases ξ is a small number and the loss is relatively insignificant.

3.3 Extension to Relaxed Inequality Conditions

We consider a generalization to the case where the condition that $P_a \neq P_b$ whenever $a \neq b$ is released to some degree. More detailed, let $\{1,\ldots,r\} = \mathcal{R}_1 \cup \cdots \cup \mathcal{R}_t$ be any partition of the r indices. We will require that $P_a \neq P_b$ whenever $a, b \in \mathcal{R}_j$ for some $j \in \{1,\ldots,t\}$. Definition 3 generalizes the obvious way in order to comply with this condition:

Definition 4 (relaxed non-degeneracy). *The system of equations $\mathcal{E}$ is* relaxed non-degenerate *with respect to partition $\{1,\ldots,r\} = \mathcal{R}_1 \cup \cdots \cup \mathcal{R}_t$ if there is no $I \subseteq \{1,\ldots,q\}$ such that the multiset $\mathcal{M}_I$ has exactly two odd multiplicity elements from a single set $\mathcal{R}_j$ ($j \in \{1,\ldots,t\}$) and such that $\bigoplus_{i\in I} \lambda_i = 0$.*

Note that a relaxed non-degenerate system of equations may induce equations of the form $P_a = P_b$ where a, b are from distinct index sets; such an equation does not make the system degenerate. The extension of Theorem 2 to relaxed inequality conditions is the following, which corresponds to [40, Theorem 7].

Theorem 3 (relaxed mirror theorem). *Let $\xi \geq 2$. Let $\{1,\ldots,r\} = \mathcal{R}_1 \cup \cdots \cup \mathcal{R}_t$ be any 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) relaxed non-degenerate with respect to partition $\{1,\ldots,r\} = \mathcal{R}_1 \cup \cdots \cup \mathcal{R}_t$. Then, as long as $(\xi-1)^2 \cdot \max_j |\mathcal{R}_j| \leq 2^n/67$, the number of solutions for $\mathcal{P}$ such that $P_a \neq P_b$ for all distinct $a, b \in \{1,\ldots,r\}$ is at least*

$$\frac{\mathrm{NonEq}(\mathcal{R}_1,\ldots,\mathcal{R}_t;\mathcal{E})}{2^{nq}},$$

where $\mathrm{NonEq}(\mathcal{R}_1,\ldots,\mathcal{R}_t;\mathcal{E})$ denotes the number of solutions to $\mathcal{P}$ that satisfy $P_a \neq P_b$ for all $a, b \in \mathcal{R}_j$ ($j = 1,\ldots,t$) as well as the inequalities imposed by $\mathcal{E}$ (but the equalities themselves released).

The quantity $\mathrm{NonEq}(\mathcal{R}_1, \ldots, \mathcal{R}_t; \mathcal{E})$ sounds rather technical, but for most systems it is fairly obvious to determine. If $P_a \oplus P_b = \lambda \neq 0$ is an equation in $\mathcal{E}$, then this equation imposes $P_a \neq P_b$; if in addition a, b are in distinct index sets, then this inequality $P_a \neq P_b$ imposes an *extra* inequality over the ones suggested by $\mathcal{R}_1, \ldots, \mathcal{R}_t$. An obvious lower bound is

$$\mathrm{NonEq}(\mathcal{R}_1, \ldots, \mathcal{R}_t; \mathcal{E}) \geq (2^n)_{|\mathcal{R}_1|}(2^n - (\xi - 1))_{|\mathcal{R}_2|} \cdots (2^n - (\xi - 1))_{|\mathcal{R}_t|} ,$$

as every unknown is in exactly one block, and this block imposes at most $\xi - 1$ additional inequalities on the unknowns. Better lower bounds can be derived for specific systems of equations. The relaxed theorem is equivalent to the original Theorem 2 if $t = 1$ and $\mathcal{R}_1 = \{1, \ldots, r\}$.

3.4 Example

The strength of the mirror theorem becomes visible by considering the sum of permutations, XoP^{p_1,p_2} of (1) and XoP'^{p} of (2). As a stepping stone to the analyses of EDM, EWCDM, and EDMD in the remainder of the paper, we prove that XoP^{p_1,p_2} is a secure PRF as long as $q \leq 2^n/67$. The proof is almost directly taken from [40] and is an immediate application of Theorem 3. Its single-key variant XoP'^{p} can be proved similarly from Theorem 2, provided $2q \leq 2^n/67$.

Proposition 1. *For any distinguisher $\mathcal{D}$ with query complexity at most $q \leq 2^n/67$, we have*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{XoP}^{p_1,p_2}}(\mathcal{D}) \leq q/2^n . \tag{12}$$

Proof. Let $p_1, p_2 \xleftarrow{\$} \mathsf{perm}(n)$ and $f \xleftarrow{\$} \mathsf{func}(n)$. Consider any fixed deterministic distinguisher $\mathcal{D}$ that has access to either $\mathcal{O} = \mathrm{XoP}^{p_1,p_2}$ (real world) or $\mathcal{P} = f$ (ideal world). It makes q construction queries recorded in a transcript $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$. Without loss of generality, we assume that $x_i \neq x_j$ whenever $i \neq j$.

In the real world, each tuple $(x_i, y_i) \in \tau$ corresponds to an evaluation of the function XoP^{p_1,p_2} and thus to evaluations $x_i \mapsto p_1(x_i)$ and $x_i \mapsto p_2(x_i)$, such that $p_1(x_i) \oplus p_2(x_i) = y_i$. Writing $P_{2i-1} := p_1(x_i)$ and $P_{2i} := p_2(x_i)$, the transcript τ defines q equations on the unknowns:

$$\begin{aligned} P_1 \oplus P_2 &= y_1 , \\ P_3 \oplus P_4 &= y_2 , \\ &\vdots \\ P_{2q-1} \oplus P_{2q} &= y_q . \end{aligned} \tag{13}$$

As $x_i \neq x_j$ whenever $i \neq j$, and additionally we use two independent permutations, all unknowns are formally distinct. In line with Sect. 3.1, denote the system of q equations of (13) by $\mathcal{E}$, and let $\mathcal{P} = \{P_1, \ldots, P_{2q}\}$ be the $2q$ unknowns. We can divide the indices $\{1,\dots,2q\}$ into two index sets: $\mathcal{R}_1 = \{1,3,\dots,2q-1\}$ are the indices corresponding to oracle p_1 and $\mathcal{R}_2 = \{2,4,\dots,2q\}$ the indices corresponding to oracle p_2.

Patarin's H-coefficient technique of Theorem 1 states that $\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{XoP}^{p_1,p_2}}(\mathcal{D}) \leq \varepsilon$, where ε is such that for any transcript τ (we do not consider bad transcripts),

$$\frac{\mathbf{Pr}\left[X_{\mathrm{XoP}^{p_1,p_2}} = \tau\right]}{\mathbf{Pr}\left[X_f = \tau\right]} \geq 1 - \varepsilon\,. \tag{14}$$

For the computation of $\mathbf{Pr}\left[X_{\mathrm{XoP}^{p_1,p_2}} = \tau\right]$ and $\mathbf{Pr}\left[X_f = \tau\right]$, it suffices to compute the probability, over the drawing of the oracles, that a good transcript is obtained. For the real world XoP^{p_1,p_2}, the transcript τ defines a system of equations $\mathcal{E}$ which is circle-free, has q blocks of size 2 (so it is 2-block-maximal), and it is relaxed non-degenerate with respect to partition $\{1,\dots,r\} = \mathcal{R}_1 \cup \mathcal{R}_2$. We can subsequently apply Theorem 3 for $\xi = 2$, and obtain that, provided $q \leq 2^n/67$, the number of solutions for the output values $\mathcal{P}$ is at least $\frac{\mathrm{NonEq}(\mathcal{R}_1,\mathcal{R}_2;\mathcal{E})}{2^{nq}}$. To lower bound $\mathrm{NonEq}(\mathcal{R}_1,\mathcal{R}_2;\mathcal{E})$, note that we have $(2^n)_q$ possible choices for $P_1, P_3, \dots, P_{2q-1}$, at least $2^n - 1$ choices for P_2 (if $y_1 \neq 0$ then P_2 should be unequal to P_1), at least $2^n - 2$ choices for P_4 (it should be unequal to P_2, and if $y_2 \neq 0$, it should moreover be unequal to P_3), etc., and we obtain

$$\mathrm{NonEq}(\mathcal{R}_1,\mathcal{R}_2;\mathcal{E}) \geq (2^n)_q (2^n-1)_q\,.$$

We have $(2^n - q)!$ possible choices for the remaining output values of p_1, and similarly of p_2. Thus,

$$\begin{aligned}\mathbf{Pr}\left[X_{\mathrm{XoP}^{p_1,p_2}} = \tau\right] &= \frac{|\{p_1,p_2 \in \mathsf{perm}(n) \mid \mathrm{XoP}^{p_1,p_2} \vdash \tau\}|}{|\mathsf{perm}(n)|^2} \\ &\geq \frac{\frac{(2^n)_q(2^n-1)_q}{2^{nq}} \cdot ((2^n-q)!)^2}{(2^n!)^2} = \frac{1}{2^{nq}}\left(1 - \frac{q}{2^n}\right)\,. \end{aligned} \tag{15}$$

For the ideal world f, we similarly obtain

$$\mathbf{Pr}\left[X_f = \tau\right] = \frac{|\{f \in \mathsf{func}(n) \mid f \vdash \tau\}|}{|\mathsf{func}(n)|} = \frac{1}{2^{nq}}\,. \tag{16}$$

We thus obtain for the ratio of (14):

$$\frac{\mathbf{Pr}\left[X_{\mathrm{XoP}^{p_1,p_2}} = \tau\right]}{\mathbf{Pr}\left[X_f = \tau\right]} \geq 1 - \frac{q}{2^n}\,.$$

We have obtained $\varepsilon = \frac{q}{2^n}$, provided $q \leq 2^n/67$. □

4 Security of EDM^{p_1,p_2}

Consider EDM of (3) for the case of independent permutations p_1, p_2. We will prove that this construction achieves close to optimal security.

Theorem 4. *Let $\xi \geq 1$ be any threshold. For any distinguisher $\mathcal{D}$ with query complexity at most $q \leq 2^n/(67\xi^2)$, we have*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{EDM}^{p_1,p_2}}(\mathcal{D}) \leq \frac{q}{2^n} + \frac{\binom{q}{\xi+1}}{2^{n\xi}}\,. \tag{17}$$

The proof will be given in the remainder of this section. It relies on the mirror theorem, although this application is not straightforward. Most importantly, rather than considering EDM^{p_1,p_2}, we consider $\mathrm{EDM}^{p_1,p_2^{-1}}$. As p_1, p_2 are mutually independent, these two constructions are provably equally secure, but it is more convenient to reason about the latter one: we can view an evaluation $y = \mathrm{EDM}^{p_1,p_2^{-1}}(x)$ as the xor of two permutations in the middle of the function, $p_1(x) \oplus p_2(y) = x$. Therefore, q evaluations of $\mathrm{EDM}^{p_1,p_2^{-1}}$ can be translated to a system of q equations on the outputs of p_1, p_2 of the form (11). Some technicalities persist, such as the fact that y may be identical for different evaluations of the construction, and make it impossible to apply the mirror theorem directly.

The ξ functions as a threshold: as long as the largest block is of size at most $\xi+1$, this means that the result of Patarin applies provided that $q \leq 2^n/(67\xi^2)$. The probability that there is a block of size $> \xi+1$ is at most $\binom{q}{\xi+1}/2^{n\xi}$. Taking $\xi = 1$ gives condition $q \leq 2^n/67$ but the bound is capped by $q^2/2^n$. The optimal choice of ξ is when $q = 2^n/(67\xi^2)$ still yields a reasonable bound, i.e., when $(67\xi^2)^{\xi+1}(\xi+1)! \geq 2^n$. For $n = 128$ this is the case for $\xi \geq 9$. For $n = 256$ this is the case for $\xi \geq 15$.

For general n, we can observe that the above definitely holds if $(67\xi^2)^\xi = 2^n$ (a better but more complicated bound can be obtained using Stirling's approximation). Solving this for ξ results in

$$\begin{aligned}
\left(67\xi^2\right)^\xi &= 2^n \\
\left(\sqrt{67}\xi\right)^\xi &= 2^{n/2} \\
\left(\sqrt{67}\xi\right)^{\sqrt{67}\xi} &= 2^{\sqrt{67}n/2} \\
\sqrt{67}\xi &= e^{W\left(\ln\left(2^{\sqrt{67}n/2}\right)\right)} \\
\frac{\ln\left(2^{\sqrt{67}n/2}\right)}{\ln\ln\left(2^{\sqrt{67}n/2}\right)} \leq \sqrt{67}\xi &\leq \frac{\ln\left(2^{\sqrt{67}n/2}\right)}{\sqrt{\ln\ln\left(2^{\sqrt{67}n/2}\right)}}\,,
\end{aligned}$$

where the last inequality comes from the approximation $\ln x - \ln\ln x \leq W(x) \leq \ln x - \frac{1}{2}\ln\ln x$ on the Lambert W function [23]. Coupled with Theorem 4, this guarantees security as long as $q \leq \frac{2^n}{(67n/\sqrt{\ln 67n})}$.

As suggested by Patarin [40, Generalization 2], it may be possible to eschew the condition $\xi^2 \cdot q \leq 2^n/67$ in favor of $\xi^2_{\mathrm{average}} \cdot q \leq 2^n/67$, where ξ_{average} denotes the average block size. For EDM^{p_1,p_2}, the probability of a given block being of size $\xi+1$ is significantly lower than of it being of size ξ; thus, the number of blocks with 2 variables is expected to dominate, and contribute the largest amount of solutions of the mirror system.

The proof of Theorem 4 consists of five steps: in Sect. 4.1 we describe how transcripts are generated, in Sect. 4.2 we discuss attainable index mappings, in Sect. 4.3 we give a definition of bad transcripts, in Sect. 4.4 we derive an upper bound on the probability of a bad transcript in the ideal world, and in Sect. 4.5 a lower bound on the ratio for good transcripts. Theorem 4 immediately follows from the H-coefficient technique of Theorem 1.

4.1 General Setting and Transcripts

Let $p_1, p_2 \xleftarrow{\$} \mathsf{perm}(n)$ and $f \xleftarrow{\$} \mathsf{func}(n)$. Consider any fixed deterministic distinguisher $\mathcal{D}$ that has access to either $\mathcal{O} = \mathrm{EDM}^{p_1,p_2^{-1}}$ (real world) or $\mathcal{P} = f$ (ideal world). It makes q construction queries recorded in a transcript $\tau = \{(x_1, y_1), \dots, (x_q, y_q)\}$. Without loss of generality, we assume that $x_i \neq x_j$ whenever $i \neq j$.

4.2 Attainable Index Mappings

In the real world, each tuple $(x_i, y_i) \in \tau$ corresponds to an evaluation of the function $\mathrm{EDM}^{p_1,p_2^{-1}}$ and thus to a one call to p_1 and one to p_2: $x_i \mapsto p_1(x_i)$ and $y_i \mapsto p_2(y_i)$, such that $p_1(x_i) \oplus p_2(y_i) = x_i$. Indeed, p_1 and p_2 xor to x_i in the middle of the function $\mathrm{EDM}^{p_1,p_2^{-1}}$. Writing $P_{a_i} := p_1(x_i)$ and $P_{b_i} := p_2(y_i)$, the transcript τ defines q equations on the unknowns:

$$\begin{aligned} P_{a_1} \oplus P_{b_1} &= x_1 \,, \\ P_{a_2} \oplus P_{b_2} &= x_2 \,, \\ &\vdots \\ P_{a_q} \oplus P_{b_q} &= x_q \,. \end{aligned} \tag{18}$$

In line with Sect. 3.1, denote the system of q equations of (18) by $\mathcal{E}$, let $\mathcal{P} = \{P_1, \dots, P_r\}$ be the r unknowns, for $r \in \{q, \dots, 2q\}$, and let

$$\varphi : \{a_1, b_1, \dots, a_q, b_q\} \to \{1, \dots, r\}$$

be the unique index mapping corresponding to the system of Eq. (18). Denote $\mathcal{R}_1 = \{\varphi(a_1), \dots, \varphi(a_q)\}$ and $\mathcal{R}_2 = \{\varphi(b_1), \dots, \varphi(b_q)\}$.

There is a relation between the index mapping and the permutations p_1, p_2, and different permutations could entail a different index mapping. Nevertheless, as $x_i \neq x_j$ whenever $i \neq j$, and additionally we consider independent permutations, any possible index mapping in the real world satisfies the following property.

Claim. $\varphi(a_i) \neq \varphi(a_j)$ if and only if $i \neq j$, and $\varphi(b_i) \neq \varphi(b_j)$ if and only if $y_i \neq y_j$. Furthermore, $\varphi(a_i) \neq \varphi(b_j)$ for any i, j.

Stated differently, φ should satisfy the input-output pattern induced by τ, and for any φ that does not satisfy this constraint, $\mathbf{Pr}\left[\varphi \mid \tau\right] = 0$. This particularly means that, if τ is given, there is a unique index mapping φ^τ (up to a reordering of the unknowns) that could have yielded the transcript. This index mapping has a range of size $q + q'$, where $q' = |\{y_1, \ldots, y_q\}| \leq q$ denotes the number of distinct range values in τ.

4.3 Bad Transcripts

In the real world, φ only exposes collisions of the form $\varphi(b_i) = \varphi(b_j)$, or equivalently $y_i = y_j$, for some i, j. As a matter of fact, multi-collisions in the range values in τ correspond to blocks in the mirror theory. Therefore, we say that a transcript τ is *bad* if there exist $\xi+1$ distinct equation indices $i_1, \ldots, i_{\xi+1} \in \{1, \ldots, q\}$ such that $y_{i_1} = \cdots = y_{i_{\xi+1}}$, where ξ is the threshold given in the theory statement.

4.4 Probability of Bad Transcripts (δ)

In accordance with Theorem 1, it suffices to analyze the probability of a bad transcript in the ideal world. We have:

$$\mathbf{Pr}\left[X_f \in \mathcal{T}_{\text{bad}}\right] = \mathbf{Pr}\left[\exists i_1, \ldots, i_{\xi+1} \in \{1, \ldots, q\} \; : \; y_{i_1} = \cdots = y_{i_{\xi+1}}\right] \leq \frac{\binom{q}{\xi+1}}{2^{n\xi}} \,,$$

where we recall that in the ideal world the randomness in the transcript τ is in the values $y_1, \ldots, y_q \xleftarrow{\$} \{0,1\}^n$. We have obtained $\delta = \frac{\binom{q}{\xi+1}}{2^{n\xi}}$.

4.5 Ratio for Good Transcripts (ε)

Recall from Sect. 4.2 that for a given transcript τ, there is a unique index mapping φ^τ that could have resulted in the transcript. Pivotal to our proof is the following lemma.

Lemma 1. *Consider good transcript τ, and denote by $\mathcal{E}$ the system of q equations corresponding to $(\varphi^\tau, x_1, \ldots, x_q)$. This system of equations is (i) circle-free, (ii) $(\xi + 1)$-block-maximal, and (iii) relaxed non-degenerate with respect to partition $\{1, \ldots, r\} = \mathcal{R}_1 \cup \mathcal{R}_2$.*

Proof. The proof relies on the fact that $\varphi^\tau(a_i) \neq \varphi^\tau(a_j)$ whenever $i \neq j$, and additionally that $\varphi^\tau(a_i) \neq \varphi^\tau(b_j)$ for any i, j. Particularly, for any $I \subseteq \{1, \ldots, q\}$ the corresponding multiset $\mathcal{M}_I$ has at least $|I|$ odd multiplicity elements, and there exists (i) no circle (Definition 1).

(ii) Suppose that $\mathcal{E}$ is not $(\xi + 1)$-block-maximal (Definition 2). Then, there exists a minimal subset $\mathcal{R} \subseteq \{1, \ldots, r\}$ of size $\geq \xi + 2$ such that for any $i \in \{1, \ldots, q\}$ we either have $\{\varphi^\tau(a_i), \varphi^\tau(b_i)\} \subseteq \mathcal{R}$ or $\{\varphi^\tau(a_i), \varphi^\tau(b_i)\} \cap \mathcal{R} = \emptyset$. Let $I \subseteq \{1, \ldots, q\}$ be the subset such that $\{\varphi^\tau(a_i), \varphi^\tau(b_i)\} \subseteq \mathcal{R}$ for all $i \in I$.

Due to our definition of φ^τ, there must be an ordering $I = \{i_1, \dots, i_{\xi+1}\}$ such that $\varphi^\tau(b_{i_1}) = \dots = \varphi^\tau(b_{i_{\xi+1}})$, or equivalently, $y_{i_1} = \dots = y_{i_{\xi+1}}$, therewith contradicting that τ is good and does not contain a $(\xi+1)$-fold collision.

(iii) Suppose that the system of equations is relaxed degenerate (Definition 4). Then, there exists a minimal subset $I \subseteq \{1, \dots, q\}$ such that the multiset $\mathcal{M}_I$ has exactly two odd multiplicity elements corresponding to the same oracle and such that $\bigoplus_{i \in I} x_i = 0$. If $|I| = 1$, then $\mathcal{M}_I$ has two elements from different oracles. If $|I| = 2$, then $\bigoplus_{i \in I} x_i \neq 0$ as the x_i are all distinct. Finally, if $|I| \geq 3$ then $\mathcal{M}_I$ has at least 3 odd multiplicity elements. □

For the computation of $\mathbf{Pr}\left[X_{\mathrm{EDM}^{p_1,p_2^{-1}}} = \tau\right]$ and $\mathbf{Pr}\left[X_f = \tau\right]$, it suffices to compute the probability, over the drawing of the oracles, that a good transcript is obtained. Starting with the real world $\mathrm{EDM}^{p_1,p_2^{-1}}$, for the transcript τ, there is a unique index mapping φ^τ. It concerns q input-output tuples of p_1 and q' input-output tuples of p_2, where $|\mathrm{rng}(\varphi^\tau)| = q + q'$. Due to Lemma 1, we can apply Theorem 3 and obtain that, provided $\xi^2 \cdot q \leq 2^n/67$, the number of solutions to these $q + q'$ unknowns is at least $\frac{\mathrm{NonEq}(\mathcal{R}_1,\mathcal{R}_2;\mathcal{E})}{2^{nq}}$. We have $(2^n - q)!$ possible choices for the remaining output values of p_1, and $(2^n - q')!$ for p_2. Thus,

$$\mathbf{Pr}\left[X_{\mathrm{EDM}^{p_1,p_2^{-1}}} = \tau\right] = \mathbf{Pr}\left[p_1, p_2 \xleftarrow{\$} \mathsf{perm}(n) \ : \ \mathrm{EDM}^{p_1,p_2^{-1}} \vdash \tau\right]$$
$$\geq \frac{\frac{\mathrm{NonEq}(\mathcal{R}_1,\mathcal{R}_2;\mathcal{E})}{2^{nq}} \cdot (2^n - q)!(2^n - q')!}{(2^n!)^2} = \frac{\mathrm{NonEq}(\mathcal{R}_1,\mathcal{R}_2;\mathcal{E})}{2^{nq}(2^n)_q(2^n)_{q'}}\,.$$

To lower bound $\mathrm{NonEq}(\mathcal{R}_1,\mathcal{R}_2;\mathcal{E})$, note that we have $(2^n)_{q'}$ possible choices for $\{P_j \mid j \in \mathcal{R}_2\}$, and subsequently at least $(2^n - 1)_q$ possible choices for $\{P_j \mid j \in \mathcal{R}_1\}$, as every index in $\mathcal{R}_1$ is in a block with exactly one unknown from $\mathcal{R}_2$. Thus,

$$\mathbf{Pr}\left[X_{\mathrm{EDM}^{p_1,p_2^{-1}}} = \tau\right] \geq \frac{(2^n - 1)_q(2^n)_{q'}}{2^{nq}(2^n)_q(2^n)_{q'}} = \frac{1}{2^{nq}}\left(1 - \frac{q}{2^n}\right)\,. \tag{19}$$

For the ideal world, we obtain

$$\mathbf{Pr}\left[X_f = \tau\right] = \mathbf{Pr}\left[f \xleftarrow{\$} \mathsf{func}(n) \ : \ f \vdash \tau\right] = \frac{1}{2^{nq}}\,. \tag{20}$$

We obtain for the ratio:

$$\frac{\mathbf{Pr}\left[X_{\mathrm{EDM}^{p_1,p_2^{-1}}} = \tau\right]}{\mathbf{Pr}\left[X_f = \tau\right]} \geq \frac{\frac{1}{2^{nq}}\left(1 - \frac{q}{2^n}\right)}{\frac{1}{2^{nq}}} = 1 - \frac{q}{2^n}\,.$$

We have obtained $\varepsilon = \frac{q}{2^n}$, provided $\xi^2 \cdot q \leq 2^n/67$.

5 Security of $\mathbf{EWCDM}^{h,p_1,p_2}$

We prove that EWCDM of (4) for the case independent permutations p_1, p_2 achieves close to optimal PRF security in the nonce-respecting setting. We remark that Cogliati and Seurin proved PRF security of $\mathrm{EWCDM}^{h,p_1,p_2}$ up to about $2^{2n/3}$ queries (cf., [17, Theorem 3] for $q_v = 0$). In a similar vein as the analysis of Cogliati and Seurin [17] on $\mathrm{EWCDM}^{h,p_1,p_2}$, our analysis straightforwardly generalizes to the analysis for unforgeability or for the nonce-misusing setting.

Theorem 5. *Let $\xi \geq 1$ be any threshold. For any distinguisher $\mathcal{D}$ with query complexity at most $q \leq 2^n/(67\xi^2)$, we have*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{EWCDM}^{h,p_1,p_2}}(\mathcal{D}) \leq \frac{q}{2^n} + \frac{\binom{q}{2}\epsilon}{2^n} + \frac{\binom{q}{\xi+1}}{2^{n\xi}}\,, \tag{21}$$

where h is an ϵ-AXU hash function.

The proof follows the same strategy as the one of EDM^{p_1,p_2}, i.e., replacing p_2 by p_2^{-1} for readability and noting that $t = \mathrm{EWCDM}^{h,p_1,p_2^{-1}}(\nu, m)$ corresponds to the xor of two permutations as $p_1(\nu) \oplus p_2(t) = \nu \oplus h(m)$. An additional hurdle has to be overcome, namely cases where $\nu \oplus h(m) = \nu' \oplus h(m')$: if this happens, and additionally we have $t = t'$, the system of equations cannot be solved. (In retrospect, one can view the proof of EDM^{p_1,p_2} as a special case of the new proof by keeping m constant.) As before, ξ functions as a threshold and the computations of Sect. 4 likewise apply.

5.1 General Setting and Transcripts

Let $h \xleftarrow{\$} H$ be an ϵ-AXU hash function, $p_1, p_2 \xleftarrow{\$} \mathsf{perm}(n)$, and $f \xleftarrow{\$} \mathsf{func}(n{+}*, n)$. Consider any fixed deterministic distinguisher $\mathcal{D}$ that has access to either $\mathcal{O} = \mathrm{EWCDM}^{h,p_1,p_2^{-1}}$ (real world) or $\mathcal{P} = f$ (ideal world). It makes q construction queries recorded in a transcript $\tau_{\mathrm{cq}} = \{(\nu_1, m_1, t_1), \ldots, (\nu_q, m_q, t_q)\}$, where the q nonces ν_i are mutually different.

We will reveal after $\mathcal{D}$'s interaction with its oracle, but before its final decision, a universal hash function h. In the real world, h is the hash function that is actually used. In the ideal world, h will be drawn uniformly at random from the ϵ-AXU universal hash function family H. The extended transcript is denoted

$$\tau = (\tau_{\mathrm{cq}}, h)\,.$$

5.2 Attainable Index Mappings

In the real world, each tuple $(\nu_i, m_i, t_i) \in \tau_{\mathrm{cq}}$ corresponds to an evaluation of the function $\mathrm{EWCDM}^{h,p_1,p_2^{-1}}$ and thus evaluations $\nu_i \mapsto p_1(\nu_i)$ and $t_i \mapsto p_2(t_i)$, such that $p_1(\nu_i) \oplus p_2(t_i) = \nu_i \oplus h(m_i)$ (note the fundamental difference with respect to the analysis of $\mathrm{EDM}^{p_1,p_2^{-1}}$ of Sect. 4, namely the addition of $h(m_i)$). Writing $P_{a_i} := p_1(\nu_i)$ and $P_{b_i} := p_2(t_i)$, the transcript τ_{cq} defines q equations on the unknowns:

$$\begin{aligned} P_{a_1} \oplus P_{b_1} &= \nu_1 \oplus h(m_1)\,, \\ P_{a_2} \oplus P_{b_2} &= \nu_2 \oplus h(m_2)\,, \\ &\vdots \\ P_{a_q} \oplus P_{b_q} &= \nu_q \oplus h(m_q)\,. \end{aligned} \tag{22}$$

(The system of equations differs from that of (18) as the unknowns should now sum to $\nu_i \oplus h(m_i)$.) In line with Sect. 3.1, denote the system of q equations of (22) by $\mathcal{E}$, let $\mathcal{P} = \{P_1, \ldots, P_r\}$ be the r unknowns, for $r \in \{q, \ldots, 2q\}$, and let

$$\varphi : \{a_1, b_1, \ldots, a_q, b_q\} \to \{1, \ldots, r\}$$

be the unique index mapping corresponding to the system of Eq. (22). Denote $\mathcal{R}_1 = \{\varphi(a_1), \ldots, \varphi(a_q)\}$ and $\mathcal{R}_2 = \{\varphi(b_1), \ldots, \varphi(b_q)\}$.

From the fact that $\nu_i \neq \nu_j$ whenever $i \neq j$, and additionally that we consider two independent permutations, we can derive the exact same property of φ as in Sect. 4.2, with ν replacing x and t replacing y.

Claim. $\varphi(a_i) \neq \varphi(a_j)$ if and only if $i \neq j$, and $\varphi(b_i) \neq \varphi(b_j)$ if and only if $t_i \neq t_j$. Furthermore, $\varphi(a_i) \neq \varphi(b_j)$ for any i, j.

As before, for a given transcript τ_{cq}, there is a unique index mapping φ^τ that could have yielded the transcript. It has a range of size $q + q'$, where $q' = |\{t_1, \ldots, t_q\}| \leq q$ denotes the number of distinct range values in τ_{cq}.

5.3 Bad Transcripts

Unlike for the analysis of $\text{EDM}^{p_1, p_2^{-1}}$, it is insufficient to just require that there is no $(\xi+1)$-fold collision, we must also take degeneracy of the system of equations into account. Indeed, if for two queries $(\nu_i, m_i, t_i), (\nu_j, m_j, t_j)$, we have that $t_i = t_j$ (or, equivalently, $\varphi(b_i) = \varphi(b_j)$) and $\nu_i \oplus h(m_i) = \nu_j \oplus h(m_j)$, the system of equations would imply that we need $\varphi(a_i) = \varphi(a_j)$, which is impossible by design.

Formally, we say that a transcript $\tau = (\tau_{\text{cq}}, h)$ is *bad* if

- there exist $\xi + 1$ distinct equation indices $i_1, \ldots, i_{\xi+1} \in \{1, \ldots, q\}$ such that $t_{i_1} = \cdots = t_{i_{\xi+1}}$, where ξ is the threshold given in the theory statement, or
- there exist two distinct equation indices $i, j \in \{1, \ldots, q\}$ such that $t_i = t_j$ and $\nu_i \oplus h(m_i) = \nu_j \oplus h(m_j)$.

5.4 Probability of Bad Transcripts (δ)

As in Sect. 4.4, it suffices to analyze the probability of a bad transcript in the ideal world, and we have:

$$\begin{aligned} \mathbf{Pr}\left[X_f \in \mathcal{T}_{\text{bad}}\right] \leq\; & \mathbf{Pr}\left[\exists i_1, \ldots, i_{\xi+1} \in \{1, \ldots, q\} \;:\; t_{i_1} = \cdots = t_{i_{\xi+1}}\right] \\ & + \mathbf{Pr}\left[\exists i, j \in \{1, \ldots, q\} \;:\; t_i = t_j \wedge \nu_i \oplus h(m_i) = \nu_j \oplus h(m_j)\right]\,, \end{aligned} \tag{23}$$

where we recall that in the ideal world the randomness in the transcript τ is in the values $t_1, \ldots, t_q \xleftarrow{\$} \{0,1\}^n$ and in the uniform drawing $h \xleftarrow{\$} H$. The first probability of (23) is identical to the one analyzed in Sect. 4.4 and upper bounded by $\binom{q}{\xi+1}/2^{n\xi}$. For the second probability of (23), there are $\binom{q}{2}$ possible indices, the first equation is satisfied with probability $1/2^n$ (due to the drawing of the t_i), and the second equation is satisfied with probability ϵ (as h is an ϵ-AXU hash function). Thus, the second probability is upper bounded by $\binom{q}{2}\epsilon/2^n$.

We thus obtain from (23):

$$\mathbf{Pr}\left[X_f \in \mathcal{T}_{\text{bad}}\right] \le \frac{\binom{q}{2}\epsilon}{2^n} + \frac{\binom{q}{\xi+1}}{2^{n\xi}} =: \delta\,.$$

5.5 Ratio for Good Transcripts (ε)

Recall from Sect. 5.2 that for a given transcript τ_{cq}, there is a unique index mapping φ^τ that could have resulted in the transcript. We can derive the following result.

Lemma 2. *Consider good transcript $\tau = (\tau_{cq}, h)$ and denote by $\mathcal{E}$ the system of q equations corresponding to $(\varphi^\tau, \nu_1 \oplus h(m_1), \ldots, \nu_q \oplus h(m_q))$. This system of equations is (i) circle-free, (ii) $(\xi+1)$-block-maximal, and (iii) relaxed non-degenerate with respect to partition $\{1, \ldots, r\} = \mathcal{R}_1 \cup \mathcal{R}_2$.*

Proof. The proof is a generalization of the one of Lemma 1. Nothing changes for circle-freeness and $(\xi+1)$-block-maximality.

Suppose that the system of equations is relaxed degenerate (Definition 4). Then, there exists a minimal subset $I \subseteq \{1, \ldots, q\}$ such that the multiset $\mathcal{M}_I$ has exactly two odd multiplicity elements corresponding to the same oracle and such that $\bigoplus_{i \in I} \nu_i \oplus h(m_i) = 0$. As in Lemma 1, this implies that $|I| = 2$, say $I = \{i, j\}$, for which $\varphi^\tau(b_i) = \varphi^\tau(b_j)$ and $\nu_i \oplus h(m_i) = \nu_j \oplus h(m_j)$, therewith contradicting that τ is good. □

The remaining analysis is almost identical to the one for $\text{EDM}^{p_1, p_2^{-1}}$ in Sect. 4.5, the sole exception being that both probabilities have an additional factor $1/|H|$, and henceforth omitted.

6 Security of EDMD^{p_1,p_2}

Consider EDMD^{p_1,p_2} of (5) for the case of independent permutations p_1, p_2. We will prove that this construction achieves optimal PRF security without a logarithmic loss.

Theorem 6. *For any distinguisher $\mathcal{D}$ with query complexity at most $q \le 2^n/67$, we have*

$$\mathbf{Adv}^{\text{prf}}_{\text{EDMD}^{p_1,p_2}}(\mathcal{D}) \le q/2^n\,. \tag{24}$$

The proof can be performed along the same lines of that of EDM^{p_1,p_2}, with the difference that for EDMD^{p_1,p_2} no collisions among the evaluations of the permutations occur. However, the exact same security bound can be derived fairly elegantly from Proposition 1.

Proof. Let $p_1, p_2, p_3 \xleftarrow{\$} \mathsf{perm}(n)$ and $f \xleftarrow{\$} \mathsf{func}(n)$. Write $\mathrm{EDMD}^{p_1,p_2} = p_2 \circ p_1 \oplus p_1$. By a simple hybrid argument we obtain:

$$\Delta(p_2 \circ p_1 \oplus p_1\ ;\ f) \leq \Delta(p_2 \circ p_1 \oplus p_1\ ;\ p_3 \oplus p_1) + \Delta(p_3 \oplus p_1\ ;\ f)\,.$$

The former distance equals 0 (reveal p_1 to the distinguisher prior to the experiment, and it effectively has to distinguish p_2 from p_3). The latter distance is bounded by $q/2^n$ provided that $q \leq 2^n/67$, cf., Proposition 1. □

7 Towards a Single Permutation

Given our results on EDM^{p_1,p_2} of Theorem 4 and EDMD^{p_1,p_2} of Theorem 6, one may expect that similar techniques apply to the case where $p_1 = p_2$. However, it seems unlikely, if not impossible, to apply the mirror theory to these constructions. The reason is that the mirror theory works particularly well if only the input values of the functions are determined, and not the output values.

For example, for EDM^{p_1,p_2}, an evaluation $y = \mathrm{EDM}^{p_1,p_2}(x)$ corresponds to evaluations $p_1(x)$ and $p_2(p_1(x) \oplus x)$, where $y = p_2(p_1(x) \oplus x)$. Thus, the query-response tuple (x, y) reveals one input value to p_1 and one output value of p_2. By, without loss of generality, replacing p_2 by its inverse we nicely obtained a system where only input values of the permutations are fixed. Now, consider EDM^p: a single evaluation $y = \mathrm{EDM}^p(x)$ reveals an input value x to p as well as an output value y of p, and there seems to be no way to properly employ the mirror theorem in this case. The trick to view $\mathrm{EDM}^{p,p^{-1}}$ does not work as the construction is not equally secure as $\mathrm{EDM}^p = \mathrm{EDM}^{p,p}$. (In fact, $\mathrm{EDM}^{p,p^{-1}}$ is trivially insecure as it maps 0 to 0.)

For the single permutation variant of EDMD, the problem appears at a different surface: the chaining. In more detail, an evaluation $y = \mathrm{EDMD}^p(x)$ corresponds to two evaluations of p: $p(x)$ and $p(p(x))$, where $y = p(x) \oplus p(p(x))$. Suppose we have a different evaluation $y' = \mathrm{EDMD}^p(x')$ such that, accidentally, $p(p(x)) = p(x')$. This implies that the permutation p necessarily satisfies the following constraints:

$$p(x) = x'\ ,\ p(p(x)) = p(x') = y \oplus x'\ ,\ p(p(x')) = y' \oplus y \oplus x'\,.$$

In other words, a collision between two evaluations of p imposes conditions on the input-output pattern of p, and the mirror theorem does not allow to handle this case nicely. (Technically, the collision in this example forms a block of size 3 in the terminology of Definition 2, but the amount of freedom we have in fixing the unknowns in the block is not 2^n (as for normal systems of equations of Sect. 3), but at most 1).

We are not aware of any potential attack on EDM^p or EDMD^p that may exploit these properties. In fact, we believe that the conjecture posed by Cogliati and Seurin [17] holds for EDM^p, and that also EDMD^p achieves optimal security. It is interesting to note that

$$\mathrm{EDM}^p \circ p = p \circ \mathrm{EDMD}^p\,,$$

and any attack on EDM^p performed by, for instance, chaining multiple evaluations of EDM^p would have its equivalent attack for EDMD^p.

Acknowledgments. Bart Mennink is supported by a postdoctoral fellowship from the Netherlands Organisation for Scientific Research (NWO) under Veni grant 016.Veni.173.017. The authors would like to thank Jacques Patarin for helpful discussions, the anonymous reviewers of CRYPTO 2017 for their useful technical comments, and Mridul Nandi for identifying an oversight in the analysis of the earlier EWCDMD construction [32].

A Proof Sketch of Theorem 2

Proof (sketch). Patarin's proof of Theorem 2 is very technical, and we only sketch its idea here. We refer to [36,40,41] for the technical details.

First consider the case of $\xi = 2$, i.e., $r = 2q$ and every unknown appears in exactly one equation. Without loss of generality (by reshuffling the unknowns), the system of equations reads

$$\mathcal{E} = \{P_1 \oplus P_2 = \lambda_1, \cdots, P_{2q-1} \oplus P_{2q} = \lambda_q\}\,. \tag{25}$$

For $u \in \{1, \ldots, q\}$, denote by $\mathcal{E}_u$ the first u equations of $\mathcal{E}$ and by h_{2u} the number of solutions to $\mathcal{E}_u$. Our target is to prove that $h_{2q} \geq \frac{(2^n)_{2q}}{2^{nq}}$, and we will prove this by induction on u. Clearly, for $u = 1$, $h_2 = 2^n$.

Suppose we have h_{2u} solutions for the first u equations. Then, h_{2u+2} counts the number of solutions to $\{P_1, \ldots, P_{2u+2}\}$ such that

- $\{P_1, \ldots, P_{2u}\}$ is a valid solution to the first u equations $\mathcal{E}_u$;
- $P_{2u+1} \oplus P_{2u+2} = \lambda_{u+1}$;
- $P_{2u+1} \notin \{P_1, \ldots, P_{2u}\} =: V_1$;
- $P_{2u+1} \notin \{P_1 \oplus \lambda_{u+1}, \ldots, P_{2u} \oplus \lambda_{u+1}\} =: V_2$.

Thus, for a given set of solutions to $\mathcal{E}_u$, we have $2^n - |V_1 \cup V_2|$ solutions for $\{P_{2u+1}, P_{2u+2}\}$. As $|V_1 \cup V_2| = |V_1| + |V_2| - |V_1 \cap V_2| = 4u - |V_1 \cap V_2|$, we obtain

$$\begin{aligned} h_{2u+2} &= \sum_{\{P_1,\ldots,P_{2u}\} \text{ solving } \mathcal{E}_u} 2^n - |V_1 \cup V_2| \\ &= \sum_{\{P_1,\ldots,P_{2u}\} \text{ solving } \mathcal{E}_u} 2^n - 4u + |V_1 \cap V_2| \\ &= (2^n - 4u)h_{2u} + \sum_{\{P_1,\ldots,P_{2u}\} \text{ solving } \mathcal{E}_u} |V_1 \cap V_2|\,. \end{aligned} \tag{26}$$

Obviously, $|V_1 \cap V_2| \geq 0$, but this gives only a poor estimation of h_{2q}, namely

$$h_{2q} \geq (2^n - 4(q-1))h_{2q-2} \geq \cdots \geq \left(\prod_{u=1}^{q-1} 2^n - 4u \right) h_2 \geq \prod_{u=0}^{q-1} 2^n - 4u\,,$$

for which

$$\begin{aligned} \frac{h_{2q} 2^{nq}}{(2^n)_{2q}} &\geq \prod_{u=0}^{q-1} \frac{(2^n - 4u)2^n}{(2^n - 2u)(2^n - 2u - 1)} \\ &= \prod_{u=0}^{q-1} 1 - \frac{-2^n + 4u^2 + 2u}{(2^n - 2u)(2^n - 2u - 1)} \\ &\geq \prod_{u=0}^{q-1} 1 - \frac{4u^2}{(2^n - 2q)^2} = 1 - O\left(\frac{q^3}{2^{2n}}\right). \end{aligned}$$

Instead, we would prefer to have a lower bound on $|V_1 \cap V_2|$ that can be used to undo the $4u^2$-term. If we could, hypothetically, prove that $|V_1 \cap V_2| \geq 4u^2/2^n$, the derivation would depart from (26) as

$$\begin{aligned} \frac{h_{2q} 2^{nq}}{(2^n)_{2q}} &\geq \prod_{u=0}^{q-1} \frac{(2^n - 4u + \frac{4u^2}{2^n})2^n}{(2^n - 2u)(2^n - 2u - 1)} \\ &= \prod_{u=0}^{q-1} 1 - \frac{-2^n + 2u}{(2^n - 2u)(2^n - 2u - 1)} \geq 1\,. \end{aligned}$$

Unfortunately, for some solutions $\{P_1, \ldots, P_{2u}\}$ satisfying $\mathcal{E}_u$, the number $|V_1 \cap V_2|$ may be well below this bound, while for others it may be much higher. Patarin proved that, in fact, a slightly worse bounding already does the job.

Rewrite the crucial quantity of (26) as

$$\sum_{\{P_1,\ldots,P_{2u}\} \text{ solving } \mathcal{E}_u} |V_1 \cap V_2| = \sum_{1 \leq i,j \leq 2u} \underbrace{\left| \left\{ \text{solutions to } \mathcal{E}_u \cup \{P_i \oplus P_j = \lambda_{u+1}\} \right\} \right|}_{=: h'_{2u}(i,j)}\,. \tag{27}$$

Denote by I_{u+1} the set of indices whose value λ_l equals λ_{u+1}, and by J_{u+1} the set of pairs of indices whose value $\lambda_l \oplus \lambda_{l'}$ equals λ_{u+1}:

$$\begin{aligned} I_{u+1} &= \{l \in \{1, \ldots, u\} \mid \lambda_l = \lambda_{u+1}\}\,, \\ J_{u+1} &= \{(l, l') \in \{1, \ldots, u\}^2 \mid \lambda_l \oplus \lambda_{l'} = \lambda_{u+1}\}\,. \end{aligned}$$

The value $h'_{2u}(i,j)$ may attain different values depending on (i,j):

- If $i, j \in \{2l-1, 2l\}$ for some $l \in \{1, \ldots, u\}$, the two unknowns come from the same equation in $\mathcal{E}_u$:

  - If $i = j$, then $h'_{2u}(i,j) = 0$, as the appended equation forms a contradiction on its own;
  - If $i \neq j$ and $l \in I_{u+1}$, then $h'_{2u}(i,j) = h_{2u}$, as the appended equation is identical to the l-th equation in $\mathcal{E}_u$, and is redundant;
  - If $i \neq j$ and $l \notin I_{u+1}$, then $h'_{2u}(i,j) = 0$, as the appended equation forms a contradiction with the l-th equation: $\lambda_l = P_i \oplus P_j = \lambda_{u+1}$;
- If $i \in \{2l-1, 2l\}$ and $j \notin \{2l-1, 2l\}$ for some $l \in I_{u+1}$, then $h'_{2u}(i,j) = 0$, as the appended equation forms a contradiction with the l-th equation. For example, if $i = 2l-1$, then the two equations imply that $P_{2l} \oplus P_j = 0$;
- If $j \in \{2l-1, 2l\}$ and $i \notin \{2l-1, 2l\}$ for some $l \in I_{u+1}$, we have $h'_{2u}(i,j) = 0$ by symmetry;
- If $i \in \{2l-1, 2l\}$ and $j \in \{2l'-1, 2l'\}$ for some $(l,l') \in J_{u+1}$, then $h'_{2u}(i,j) = 0$, as the l-th, l'-th, and appended equation form a contradiction. For example, if $i = 2l-1$ and $j = 2l'-1$, then the three equations imply that $P_{2l} = P_{2l'}$;
- If neither of the above applies, we are in the hard case. Denote by M_{u+1} the set of indices covered by this case:

$$\begin{aligned} M_{u+1} = \Big\{(i,j) \in \{1,\ldots,2u\}^2\Big\} \Big\backslash \\ &\Big\{(2l-1,2l-1),(2l-1,2l),(2l,2l-1),(2l,2l) \;\Big|\; l \in \{1,\ldots,u\}\Big\} \cup \\ &\Big\{(2l-1,*),(2l,*),(*,2l-1),(*,2l) \;\Big|\; l \in I_{u+1}\Big\} \cup \\ &\Big\{(2l-1,2l'-1),(2l-1,2l'),(2l,2l'-1),(2l,2l') \;\Big|\; (l,l') \in J_{u+1}\Big\}\,. \end{aligned}$$

Effectively, we have obtained from (26) and (27) that

$$\begin{aligned} h_{2u+2} &= (2^n - 4u)h_{2u} + \sum_{1 \le i,j \le 2u} h'_{2u}(i,j) \\ &= (2^n - 4u)h_{2u} + 2|I_{u+1}|h_{2u} + \sum_{(i,j) \in M_{u+1}} h'_{2u}(i,j)\,. \end{aligned} \tag{28}$$

Patarin proves the following two claims.

Claim (Patarin [40, *Theorem* 10]*).* $|M_{u+1}| \ge 4u^2 - 8u - 12|I_{u+1}|u$.
Claim (Patarin [40, *Theorem* 18]*).* For any $(i,j) \in M_{u+1}$, provided $2u \le 2^n/32$,[4]

$$h'_{2u}(i,j) \ge \frac{h_{2u}}{2^n}\left(1 - \frac{124u}{2^{2n}} - \frac{104|I_{u+2}|u}{2^{2n}}\right).$$

The former claim relies on the observation that, without loss of generality, the equations are ordered in such a way that λ_{u+1} is the most-frequent value so far. The second claim captures the technical heart of the result. From (28) and above two claims, we derive

$$\begin{aligned} \frac{h_{2u+2}}{h_{2u}} &\ge 2^n - 4u + 2|I_{u+1}| + \frac{4u^2 - 8u - 12|I_{u+1}|u}{2^n}\left(1 - \frac{124u}{2^{2n}} - \frac{104|I_{u+2}|u}{2^{2n}}\right) \\ &\ge 2^n - 4u + 2|I_{u+1}| + \frac{4u^2 - 8u - 12|I_{u+1}|u}{2^n} - \frac{4u^2}{2^n}\left(\frac{124u}{2^{2n}} + \frac{104|I_{u+2}|u}{2^{2n}}\right), \end{aligned}$$

[4] Closer inspection of the proof reveals that $2u \le 2^n/16$ suffices.

and subsequently,

$$\begin{aligned}
&\frac{h_{2u+2}}{h_{2u}} \cdot \frac{2^n}{(2^n-2u)(2^n-2u-1)}\\
&\geq \frac{2^{2n} - 4u2^n + 2|I_{u+1}|2^n + 4u^2 - 8u - 12|I_{u+1}|u - 4u^2\left(\frac{124u}{2^{2n}} + \frac{104|I_{u+2}|u}{2^{2n}}\right)}{(2^n-2u)(2^n-2u-1)}\\
&= 1 + \frac{\left(2^n - 10u - \frac{496u^3}{2^{2n}}\right) + |I_{u+1}|\left(2\cdot 2^n - 12u - \frac{416u^3}{2^{2n}}\right)}{(2^n-2u)(2^n-2u-1)}\\
&\overset{\star}{\geq} 1 + \frac{2^n - 10u - \frac{496u^3}{2^{2n}}}{(2^n-2u)(2^n-2u-1)} \overset{\star\star}{\geq} 1\,,
\end{aligned}$$

where $\overset{\star}{\geq}$ holds for $2u \leq 2^n/5$ and $\overset{\star\star}{\geq}$ under the condition that $2u \leq 2^n/7$.[5] Note that the bounding is done on $2u$ rather than u: we are currently still looking at the case of $\xi = 2$, and every block has 2 unknowns. The condition states an upper bound on the number of unknowns.

The bound $h_{2u+2}/h_{2u} \geq 1$ holds for any $u = 2, \ldots, q-1$. As, in addition, $h_2 = 2^n$, we derive

$$h_{2q} \geq \frac{(2^n-2q+1)(2^n-2q+2)}{2^n} h_{2q-2} \geq \cdots \geq \frac{(2^n-2)_{2q-2}}{2^{n(q-1)}} h_2 \geq \frac{(2^n)_{2q}}{2^{nq}}\,,$$

as long as $2(q-1) \leq 2^n/32$. This completes the proof.

The induction step in the proof is performed over the number of equations, and every step implicitly goes per two: two new unknowns are fixed and they should not hit any of the previously fixed unknowns. If we generalize this to systems of equations with larger values of ξ and where the blocks may be of different sizes, the induction would go over the number of blocks, and the size of every step corresponds to the number of unknowns in that block. This also results in more constraints *per induction step*.

For example, consider a system of equations $\mathcal{E}$, consisting of q' *blocks*. For $u \in \{1, \ldots, q'\}$ denote by $\mathcal{E}_u$ all equations that correspond to the first u blocks. If the first u blocks in total cover $v(u)$ unknowns, the value $h_{v(u)}$ is similarly defined as the number of solutions to $\mathcal{E}_u$. Suppose we have fixed the first $v(u)$ unknowns over the first u blocks, and consider a new block of ξ unknowns: the target is to determine $h_{v(u+1)} = h_{v(u)+\xi}$ from $h_{v(u)}$. Denote $v := v(u)$ for brevity. As $P_{v+1}, \ldots, P_{v+\xi}$ are in the same block, all values are fixed through the $\mathcal{E}_{u+1}$ once P_{v+1} is fixed: say that the system fixes $P_{v+i} = P_{v+1} \oplus \lambda'_i$ for some λ'_i, for $i = 2, \ldots, \xi$. (In the specific case of $\xi = 2$ treated before, $v = 2u$ and $\lambda'_2 = \lambda_{u+1}$.)

[5] We remark that Patarin derived upper bound $2^n/67$: he stated the claim on $h'_{2u}(i,j)$ for unknown constants, subsequently derived the side condition, and only then derived the constants (and hence the 67). Knowing the constants in retrospect allows us to obtain a better bounding. In the end, the side condition in the theorem statement is the most dominant one (the one of the second claim).

The value $h_{v+\xi}$ counts the number of solutions $\{P_1, \ldots, P_v, P_{v+1}, \ldots, P_{v+\xi}\}$ such that

- $\{P_1, \ldots, P_v\}$ is a valid solution to the first u *blocks* $\mathcal{E}_u$;
- $\{P_{v+1}, \ldots, P_{v+\xi}\}$ satisfy the $(u+1)$-th block $\mathcal{E}_{u+1} \backslash \mathcal{E}_u$;
- $P_{v+1} \notin \{P_1, \ldots, P_v\} =: V_1$;
- $P_{v+1} \notin \{P_1 \oplus \lambda'_2, \ldots, P_v \oplus \lambda'_2\} =: V_2$;
- $\ldots$;
- $P_{v+1} \notin \{P_1 \oplus \lambda'_\xi, \ldots, P_v \oplus \lambda'_\xi\} =: V_\xi$.

Note that the values $\{P_{v+1}, \ldots, P_{v+\xi}\}$ are distinct by hypothesis on the system of equations, or stated differently, $\lambda'_i \neq \lambda'_j \neq 0$ for any $i \neq j$. Now, in this generalized case, for a given set of solutions to $\mathcal{E}_u$, we have $2^n - |V_1 \cup \cdots \cup V_\xi|$ solutions for $\{P_{v+1}, \ldots, P_{v+\xi}\}$. By the inclusion-exclusion principle,

$$\begin{aligned} |V_1 \cup \cdots \cup V_\xi| &= \sum_{i=1}^{\xi} |V_i| - \sum_{j=2}^{\xi} (-1)^j \sum_{i_1 < \cdots < i_j} |V_{i_1} \cap \cdots \cap V_{i_j}| \\ &= \xi \cdot v - \sum_{j=2}^{\xi} (-1)^j \sum_{i_1 < \cdots < i_j} |V_{i_1} \cap \cdots \cap V_{i_j}| \,, \end{aligned}$$

from which

$$\begin{aligned} h_{v+\xi} &= \sum_{\{P_1,\ldots,P_v\} \text{ solving } \mathcal{E}_u} 2^n - |V_1 \cup \cdots \cup V_\xi| \\ &= \sum_{\{P_1,\ldots,P_v\} \text{ solving } \mathcal{E}_u} 2^n - \xi \cdot v + \sum_{j=2}^{\xi} (-1)^j \sum_{i_1 < \cdots < i_j} |V_{i_1} \cap \cdots \cap V_{i_j}| \\ &= (2^n - \xi \cdot v) h_v + \sum_{\{P_1,\ldots,P_v\} \text{ solving } \mathcal{E}_u} \sum_{j=2}^{\xi} (-1)^j \sum_{i_1 < \cdots < i_j} |V_{i_1} \cap \cdots \cap V_{i_j}| \,. \end{aligned} \tag{29}$$

Instead of the quantity of (27), it now requires to lower bound

$$\sum_{\{P_1,\ldots,P_v\} \text{ solving } \mathcal{E}_u} \sum_{j=2}^{\xi} (-1)^j \sum_{i_1 < \cdots < i_j} |V_{i_1} \cap \cdots \cap V_{i_j}| \,,$$

which is beyond the scope of the sketch of the proof. What is important to note is the term $\xi \cdot v$ in (29), which demonstrates an additional loss compared to the $4u$ in (26) for the case where all blocks are of size $\xi = 2$ unknowns. This loss, among others, eventually constitutes a stronger side condition. □

References

1. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404 (2013)
2. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The SKINNY family of block ciphers and its low-latency variant MANTIS. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9815, pp. 123–153. Springer, Heidelberg (2016). doi:10.1007/978-3-662-53008-5_5
3. Bellare, M., Impagliazzo, R.: A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. Cryptology ePrint Archive, Report 1999/024 (1999)
4. Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A concrete security treatment of symmetric encryption. In: FOCS 1997, pp. 394–403. IEEE Computer Society (1997)
5. Bellare, M., Guérin, R., Rogaway, P.: XOR MACs: new methods for message authentication using finite pseudorandom functions. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 15–28. Springer, Heidelberg (1995). doi:10.1007/3-540-44750-4_2
6. Bellare, M., Kilian, J., Rogaway, P.: The security of cipher block chaining. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 341–358. Springer, Heidelberg (1994). doi:10.1007/3-540-48658-5_32
7. Bellare, M., Krovetz, T., Rogaway, P.: Luby-Rackoff backwards: increasing security by making block ciphers non-invertible. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 266–280. Springer, Heidelberg (1998). doi:10.1007/BFb0054132
8. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 409–426. Springer, Heidelberg (2006). doi:10.1007/11761679_25
9. Bernstein, D.J.: How to stretch random functions: the security of protected counter sums. J. Cryptology **12**(3), 185–192 (1999)
10. Bhargavan, K., Leurent, G.: On the practical (in-)security of 64-bit block ciphers: Collision attacks on HTTP over TLS and OpenVPN. In: Weippl, E.R., Katzenbeisser, S., Kruegel, C., Myers, A.C., Halevi, S. (eds.) ACM SIGSAC. pp. 456–467. ACM (2016)
11. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007). doi:10.1007/978-3-540-74735-2_31
12. Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S.S., Yalçın, T.: PRINCE – a low-latency block cipher for pervasive computing applications. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 208–225. Springer, Heidelberg (2012). doi:10.1007/978-3-642-34961-4_14
13. Chang, D., Nandi, M.: A short proof of the PRP/PRF switching lemma. Cryptology ePrint Archive, Report 2008/078 (2008)
14. Chen, S., Lampe, R., Lee, J., Seurin, Y., Steinberger, J.: Minimizing the two-round even-mansour cipher. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 39–56. Springer, Heidelberg (2014). doi:10.1007/978-3-662-44371-2_3

15. Chen, S., Steinberger, J.: Tight security bounds for key-alternating ciphers. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 327–350. Springer, Heidelberg (2014). doi:10.1007/978-3-642-55220-5_19
16. Cogliati, B., Lampe, R., Patarin, J.: The indistinguishability of the XOR of k permutations. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 285–302. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46706-0_15
17. Cogliati, B., Seurin, Y.: EWCDM: an efficient, beyond-birthday secure, nonce-misuse resistant MAC. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9814, pp. 121–149. Springer, Heidelberg (2016). doi:10.1007/978-3-662-53018-4_5
18. Cannière, C., Dunkelman, O., Knežević, M.: KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers. In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol. 5747, pp. 272–288. Springer, Heidelberg (2009). doi:10.1007/978-3-642-04138-9_20
19. Gilboa, S., Gueron, S.: The advantage of truncated permutations. CoRR abs/1610.02518 (2016)
20. Gong, Z., Nikova, S., Law, Y.W.: KLEIN: a new family of lightweight block ciphers. In: Juels, A., Paar, C. (eds.) RFIDSec 2011. LNCS, vol. 7055, pp. 1–18. Springer, Heidelberg (2012). doi:10.1007/978-3-642-25286-0_1
21. Hall, C., Wagner, D., Kelsey, J., Schneier, B.: Building PRFs from PRPs. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 370–389. Springer, Heidelberg (1998). doi:10.1007/BFb0055742
22. Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B.-S., Lee, C., Chang, D., Lee, J., Jeong, K., Kim, H., Kim, J., Chee, S.: HIGHT: a new block cipher suitable for low-resource device. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 46–59. Springer, Heidelberg (2006). doi:10.1007/11894063_4
23. Hoorfar, A., Hassani, M.: Inequalities on the Lambert W function and hyperpower function. J. Inequalities Pure Appl. Math. **9**(2), 5–9 (2008)
24. Impagliazzo, R., Rudich, S.: Limits on the provable consequences of one-way permutations. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 8–26. Springer, New York (1990). doi:10.1007/0-387-34799-2_2
25. Iwata, T.: New blockcipher modes of operation with beyond the birthday bound security. In: Robshaw, M. (ed.) FSE 2006. LNCS, vol. 4047, pp. 310–327. Springer, Heidelberg (2006). doi:10.1007/11799313_20
26. Iwata, T., Mennink, B., Vizár, D.: CENC is optimally secure. Cryptology ePrint Archive, Report 2016/1087 (2016)
27. Lim, C.H., Korkishko, T.: mCrypton – a lightweight block cipher for security of low-cost RFID tags and sensors. In: Song, J.-S., Kwon, T., Yung, M. (eds.) WISA 2005. LNCS, vol. 3786, pp. 243–258. Springer, Heidelberg (2006). doi:10.1007/11604938_19
28. Luby, M., Rackoff, C.: How to construct pseudorandom permutations from pseudorandom functions. SIAM J. Comput. **17**(2), 373–386 (1988)
29. Lucks, S.: The sum of PRPs is a secure PRF. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 470–484. Springer, Heidelberg (2000). doi:10.1007/3-540-45539-6_34
30. Mennink, B., Preneel, B.: On the XOR of multiple random permutations. In: Malkin, T., Kolesnikov, V., Lewko, A.B., Polychronakis, M. (eds.) ACNS 2015. LNCS, vol. 9092, pp. 619–634. Springer, Cham (2015). doi:10.1007/978-3-319-28166-7_30
31. Nachef, V., Patarin, J., Volte, E.: Feistel Ciphers - Security Proofs and Cryptanalysis. Springer, Cham (2017). doi:10.1007/978-3-319-49530-9

32. Nandi, M.: Birthday attack on dual EWCDM. Cryptology ePrint Archive, Report 2017/579 (2017)
33. Patarin, J.: Étude des Générateurs de Permutations Basés sur le Schéma du D.E.S. Ph.D. thesis, Université Paris 6, Paris, France, November 1991
34. Patarin, J.: Luby-Rackoff: 7 rounds are enough for $2^{n(1-\epsilon)}$ security. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 513–529. Springer, Heidelberg (2003). doi:10.1007/978-3-540-45146-4_30
35. Patarin, J.: Security of random feistel schemes with 5 or more rounds. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 106–122. Springer, Heidelberg (2004). doi:10.1007/978-3-540-28628-8_7
36. Patarin, J.: On linear systems of equations with distinct variables and small block size. In: Won and Kim [49], pp. 299–321 (2006)
37. Patarin, J.: The "Coefficients H" Technique. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 328–345. Springer, Heidelberg (2009). doi:10.1007/978-3-642-04159-4_21
38. Patarin, J.: A proof of security in $O(2^n)$ for the benes scheme. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 209–220. Springer, Heidelberg (2008). doi:10.1007/978-3-540-68164-9_14
39. Patarin, J.: A proof of security in $O(2^n)$ for the XOR of two random permutations. In: Safavi-Naini, R. (ed.) ICITS 2008. LNCS, vol. 5155, pp. 232–248. Springer, Heidelberg (2008). doi:10.1007/978-3-540-85093-9_22
40. Patarin, J.: Introduction to mirror theory: analysis of systems of linear equalities and linear non equalities for cryptography. Cryptology ePrint Archive, Report 2010/287 (2010)
41. Patarin, J.: Security of balanced and unbalanced Feistel schemes with linear non equalities. Cryptology ePrint Archive, Report 2010/293 (2010)
42. Patarin, J.: Security in $O(2^n)$ for the xor of two random permutations. Proof with the standard H technique. Cryptology ePrint Archive, Report 2013/368 (2013)
43. Patarin, J.: Mirror theory and cryptography. Cryptology ePrint Archive, Report 2016/702 (2016)
44. Patarin, J.: Personal communication (2017)
45. Patarin, J., Montreuil, A.: Benes and butterfly schemes revisited. In: Won and Kim [49], pp. 92–116 (2009)
46. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., Shirai, T.: *Piccolo*: an ultra-lightweight blockcipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 342–357. Springer, Heidelberg (2011). doi:10.1007/978-3-642-23951-9_23
47. Stam, A.J.: Distance between sampling with and without replacement. Stat. Neerl. **32**(2), 81–91 (1978)
48. Volte, E.: Miroirs, Cubes et Feistel Dissymétriques. (Mirrors, cubes and unbalanced Feistel schemes). Ph.D. thesis, Cergy-Pontoise University, France (2014)
49. Volte, E., Nachef, V., Marrière, N.: Automatic expectation and variance computing for attacks on Feistel schemes. Cryptology ePrint Archive, Report 2016/136 (2016)
50. Won, D.H., Kim, S. (eds.): ICISC 2005. LNCS, vol. 3935. Springer, Heidelberg (2006)
51. Wu, W., Zhang, L.: LBlock: a lightweight block cipher. In: Lopez, J., Tsudik, G. (eds.) ACNS 2011. LNCS, vol. 6715, pp. 327–344. Springer, Heidelberg (2011). doi:10.1007/978-3-642-21554-4_19