# Security Definitions For Hash Functions: Combining UCE and Indifferentiability*

Daniel Jost  Ueli Maurer

Department of Computer Science, ETH Zurich, Switzerland
daniel.jost@inf.ethz.ch
maurer@inf.ethz.ch

**Abstract**

Hash functions are one of the most important cryptographic primitives, but their desired security properties have proven to be remarkably hard to formalize. To prove the security of a protocol using a hash function, nowadays often the random oracle model (ROM) is used due to its simplicity and its strong security guarantees. Moreover, hash function constructions are commonly proven to be secure by showing them to be indifferentiable from a random oracle when using an ideal compression function. However, it is well known that no hash function realizes a random oracle and no real compression function realizes an ideal one.

As an alternative to the ROM, Bellare et al. recently proposed the notion of universal computational extractors (UCE). This notion formalizes that a family of functions "behaves like a random oracle" for "real-world" protocols while avoiding the general impossibility results. However, in contrast to the indifferentiability framework, UCE is formalized as a multi-stage game without clear composition guarantees.

As a first contribution, we introduce context-restricted indifferentiability (CRI), a generalization of indifferentiability that allows us to model that the random oracle does not compose generally but can only be used within a well-specified set of protocols run by the honest parties, thereby making the provided composition guarantees explicit. We then show that UCE and its variants can be phrased as a special case of CRI. Moreover, we show how our notion of CRI leads to generalizations of UCE. As a second contribution, we prove that the hash function constructed by Merkle-Damgård satisfies one of the well-known UCE variants, if we assume that the compression function satisfies one of our generalizations of UCE, basing the overall security on a plausible assumption. This result further validates the Merkle-Damgård construction and shows that UCE-like assumptions can serve both as a valid reference point for modular protocol analyses, as well as for the design of hash functions, linking those two aspects in a framework with explicit composition guarantees.

*This is the full version of the article due to appear at SCN 2018. The final publication will be available at link.springer.com

# Contents

**1 Introduction** **3**
1.1 Motivation and Background . . . 3
1.2 Contributions . . . 3
1.3 Related Work . . . 4

**2 Preliminaries** **5**
2.1 The (Traditional) UCE framework . . . 5
2.2 Resources and Converters . . . 6
2.3 Indifferentiability . . . 7

**3 Context-Restricted Indifferentiability** **8**
3.1 The Limitations of General Composability . . . 8
3.2 Context-Restriction . . . 9
3.3 Composition . . . 10
3.4 Relation to Indifferentiability . . . 11
3.5 An Example of CRI: Diffie-Hellman Key Exchange . . . 12

**4 Modeling UCE in CRI** **13**
4.1 Applying CRI to the ROM . . . 13
4.2 Non-Interactive Contexts . . . 14
4.3 ROM-CRI Security Implies UCE Security . . . 15

**5 Modeling Public-Seed Pseudorandom Permutations in CRI** **16**
5.1 Public-Seed Pseudorandomness . . . 17
5.2 Ideal Primitives and Function Families in CRI . . . 18
5.3 CRI-Security Implies psPR-Security . . . 18

**6 Generalizing Split-Security** **19**
6.1 Split-Security . . . 19
6.2 An Alternative Representation of Split-Security . . . 19
6.3 Strong-Split security . . . 21
6.4 Strict Min-Entropy Seeds . . . 22
6.5 The Repeated Split-Source Context Set . . . 24
6.6 The Relation Between ICE and Strong-Split CRI . . . 25

**7 Split-Security of the Merkle-Damgård Construction** **26**
7.1 Motivation . . . 26
7.2 Formalizing the Theorem . . . 26
7.3 Proof of Theorem 7.3 . . . 27
7.4 A Sufficient Condition Based on Min-Entropy Splitting . . . 30

**8 Conclusion** **32**

**A Proof of Lemma 6.8** **32**

**References** **36**

# 1 Introduction

## 1.1 Motivation and Background

The random oracle model (ROM) [BR93] is an important tool towards establishing confidence in the security of real-world cryptographic constructions. The paradigm can be described in two steps: first, to design a protocol and prove it secure in the ROM, thus using a random oracle instead of a hash function; second, to instantiate the random oracle with a cryptographic hash function. However, it is well known [CGH04] that no hash function realizes a random oracle; hence, once the random oracle is instantiated the security proof degenerates to a heuristic security argument.

The ROM is not only used as a model to prove protocols in, but it also serves as a reference point for the designers of hash functions. The indifferentiability framework [MRH04], while being a general framework, is most famously used to phrase the security obligation of a hash function construction: the hash function is proven indifferentiable from a random oracle when using an ideal compression function (e.g. a fixed input-length random oracle), thereby excluding attacks exploiting the construction. Since indifferentiability is equipped with a composition theorem, this guarantee holds moreover irrespective of the context the hash function is used in. However, just as no hash function can instantiate a random oracle, no real compression function can instantiate the idealized version assumed in the proof.

More recently, Bellare et al. [BHK14] proposed the notion of *universal computational extractors (UCE)*. This notion is based on the observation that for most "real-world" protocols proven secure in the random oracle model, instantiating the random oracle with a concrete hash function is not known to be insecure. The UCE framework revisits the question of what it means for a hash functions to "behave like a random oracle" and formalizes families of security notions aimed at bridging the gap between the general impossibility result and the apparent security of concrete protocols. So far, the research on the UCE framework has mainly been focused on two aspects: first, studying in which applications the ROM can be safely replaced by one of the UCE assumptions and, second, studying which ones of the UCE assumptions are generally uninstantiable and which one might actually be. Little attention, however, has been paid analyzing common hash function constructions within the UCE framework. Moreover, UCE is formalized as a multi-stage game without clear composition guarantees, which makes it therefore hard to directly apply as a modular step in an analysis of a complex protocol.

## 1.2 Contributions

Our contributions are three-fold. First, we introduce a (parametrized) generalization of indifferentiability called *context-restricted indifferentiability (CRI)*. This generalization allows us to model that a resource cannot be instantiated in every context but only within a well-specified set of contexts. Formally, CRI consists of a family of statements, of which classical indifferentiability is the strongest one, i.e., we weaken indifferentiability to avoid impossibility results while maintaining explicit composition guarantees. We then mainly apply the general context-restricted indifferentiability framework to the random oracle, called *random-oracle context-restricted indifferentiability (RO-CRI)* security.

Secondly, we show that every UCE-class, i.e., every variant of the original UCE framework introduced by Bellare et al., can be expressed as a set of non-interactive contexts in which the random oracle can be instantiated. Hence, we prove that the

UCE framework can be translated to RO-CRI and, thus, is essentially a special case of it. Thereby we propose an alternative interpretation of the UCE framework in a traditional single-stage adversary model with well-defined composition guarantees and provide a direct relation between the UCE and the indifferentiability frameworks. We furthermore show how two of the generalizations of UCE can be expressed within RO-CRI as well. Viewing UCE as a special case of CRI then allows us to generalize the split-source UCE-class to non-interactive contexts and we propose in particular a generalization that we call strong-split security.

Finally, we propose to consider CRI to analyze the security of common hash-function constructions. In contrast to indifferentiability, CRI allows us to consider more fine-grained versions of both the assumption on the compression function as well as the guarantee of the constructed hash function. As an example, we investigate the split-security of the Merkle-Damgård scheme using RO-CRI and we prove that the constructed hash function is split-secure if the underlying compression function is strong-split secure (as opposed to the usual much stronger assumption of the compression function being a random function) if the hashed message has a sufficient min-entropy density from the distinguisher's point of view. We thereby generalize a lemma on min-entropy splitting by Damgård et al., which we believe might be of independent interest.

### 1.3 Related Work

We discuss the relation between context-restricted indifferentiability and some related notions, including variants of indifferentiability and UCE.

**Variants of Indifferentiability.** Several variants of indifferentiability have been proposed in the past. The reset indifferentiability notion has been introduced by Ristenpart, Shacham, and Shrimpton in [RSS11] as a workaround to the composition problems in multi-stage settings they highlighted. In [DGHM13], Demay et al. gave an alternative interpretation of those shortcomings. They prove that reset indifferentiability is equivalent to indifferentiability with stateless simulators. Moreover, they introduce the notion of resource-restricted indifferentiability, which makes the memory used in the simulator explicit in contrast to the original definition which only requires this memory to be polynomially bounded. In contrast to our CRI notion that weakens indifferentiability, those two variants are a strengthening, i.e., any statement in those frameworks implies the traditional indifferentiability statement, but not vice-versa.

In [Mit14], Mittelbach presents a condition called unsplittability on multi-stage games, that allows to show that the composition theorem of indifferentiability can be salvaged for iterative hash function constructions. They formalize a condition that specifies certain multi-stage games, in which the random oracle can be safely instantiated by an iterated hash function based on an idealized compression function. In contrast, CRI formalizes in which single-stage settings a hash function might be instantiable by an actual hash function, without having to assume an unrealistically ideal compression function. Moreover, CRI is a general paradigm that not only applies to iterative hash function constructions.

**Universal Computation Extractors and Variants Thereof.** The UCE framework was introduced by Bellare et al. [BHK13] as a tool to provide a family of notions of security for keyed hash functions, refining the predominant random oracle methodology. Since then, the impossibility of various UCE-classes has been shown by

Brzuska et al. [BFM14; BM15] and Bellare et al. [BST16], and the possibility of a specific UCE-class in the standard model has been shown by Brzuska and Mittelbach [BM14]. Bellare et al. [BHK14] have also suggested to use the UCE framework to study the domain extension of a finite input-length random oracle to a UCE secure variable input-length random oracle. Their motivation is based on finding more efficient constructions if they only require the UCE-security of the variable input-length random oracle. In constrast, we consider the domain extension in a setting where we also assume the compression function to be only UCE secure.

In [FM16], Farshim and Mittelbach introduced a generalization of UCE called interactive computational extractors (ICE). Generalizing UCE to interactive scenarios is also one of our contributions. The generalization they propose and the one we propose, however, differ on a very fundamental level and pursue different directions. ICE makes the two stages of the original UCE definition symmetrical where the two stages jointly form the queries, requiring that neither one of them can predict the query. In contrast, we exactly use the asymmetry of UCE to embed it in the traditional indifferentiability setting with one dishonest and one honest party, where naturally the honest party knows the position where it queries the hash function.

In [ST17], Soni and Tessaro introduce the notion of public-seed pseudorandom permutations (psPRP) that are inspired by UCE. In fact, they introduce a generalization of UCE, called public-seed pseudorandomness, of which both psPRP and UCE are instantiations. For their psPRP notion they introduce the unpredictability and reset-security notions analogous to UCE, and moreover they study the relations between psPRP and UCE. In contrast to CRI, their definition is still purely game-based. In Section 5, we show that CRI is a strict generalization of their notion as well.

## 2 Preliminaries

### 2.1 The (Traditional) UCE framework

To circumvent the well-known impossibility result that no hash function family is indifferentiable from a random oracle, Bellare, Hoang, and Keelveedhi [BHK14] introduced the UCE framework to formalize a weaker version of what it means for a family of keyed hash functions to behave like a random oracle. The UCE framework defines a two-stage adversary, where only the first stage—the *source* $S$—has access to the oracle (either the hash function or the random oracle) and only the second stage—the *distinguisher* $D$—has access to the hash key $hk$. The source provides some *leakage* $L$ to the distinguisher that then decides with which system the source interacted. The definition of the security game is presented in Figure 1. Here, H.Kg denotes the key-generation algorithm, H.Ev the deterministic evaluation algorithm, and $l$ the output length associated with the family of hash functions $H$.

Without any further restriction, this game is trivial to win: the source queries some point $x$, obtains the result $y$, and then provides the tuple $(x, y)$ as leakage to the distinguisher which then decides whether $y$ matches with the hash of $x$. Therefore, in order for this definition to be meaningful, the leakage has to be restricted in some sense, which gives rise to various *UCE-classes* depending on the kind of restriction. The basic restriction proposed was that the queries of the source $S$ must be unpredictable given the leakage $L$. Both statistical unpredictability as well as computational unpredictability have been proposed; however, the latter has been shown to be impossible assuming iO exists [BFM14].

**Algorithm 1** The UCE game

**function** MAIN $\text{UCE}_H^{S,D}(\lambda)$
  $b \xleftarrow{\$} \{0,1\}$; $hk \xleftarrow{\$} \text{H.Kg}(1^\lambda)$
  $L \xleftarrow{\$} S^{\text{HASH}}(1^\lambda)$
  $b' \xleftarrow{\$} D(1^\lambda, hk, L)$
  **return** $(b' = b)$

**function** HASH$(x, 1^l)$
  **if** $T[x,l] = \perp$ **then**
    **if** $b = 1$ **then**
      $T[x,l] \leftarrow \text{H.Ev}(1^\lambda, hk, x, 1^l)$
    **else** $T[x,l] \xleftarrow{\$} \{0,1\}^l$
  **return** $T[x,l]$

Figure 1: The UCE game for a hash function $H$, a source $S$, and a distinguisher $D$.

## 2.2 Resources and Converters

The indifferentiability framework by Maurer, Renner, and Holenstein [MRH04] is a widely adopted framework to analyze and prove the security of hash function constructions. The indifferentiability framework is a simulation-based framework that uses the so-called "real world – ideal world" paradigm and formalizes security guarantees as resources (analogous to functionalities in the Universal Composability framework [Can01]). A resource $\mathsf{S}$ captures the idea of a module which provides some well-defined functionality to the different parties–both the honest and the dishonest ones–which can then be used in a higher level protocol. A resource can either be something physically available, such as an insecure communication network, or can be constructed from another resource $\mathsf{R}$ using a cryptographic protocol $\pi$. In fact, the goal of the protocol $\pi$ can be seen as constructing the ideal resource $\mathsf{S}$ from the real one $\mathsf{R}$ assumed to be available. The protocol is modeled as a converter that connects to the system $\mathsf{R}$.

The indifferentiability framework formalizes this concept in a setting with a single honest and a single dishonest party. In the following we give a brief description of the system algebra used in this work. We basically follow the contemporary notation of indifferentiability presented in [MR16], while sticking to the original reducibility notion.

**Formal definitions.** A resource is a system with two interfaces via which the resource interacts with its environment. The (private) interface `A` and the (public) interface `E` can be thought as being assigned to an honest and a dishonest party, respectively. Let $\Phi$ denote the set of resources. All resources in $\Phi$ are *outbound* (as in the original version of indifferentiability) meaning that interaction at one interface does not influence the other interface. If two resources $\mathsf{V}$ and $\mathsf{W}$ are used in parallel, this is again a resource, denoted $[\mathsf{V}, \mathsf{W}]$, where each of the interfaces allows to access the corresponding interfaces of both subsystems. Moreover, we assume the existence of a resource $\square \in \Phi$ such that $[\mathsf{R}, \square] = \mathsf{R}$ for any $\mathsf{R}$.

Converters are systems that can be connected to an interface of a resource to translate the inputs and outputs. A converter has two interfaces: the outer interface `out` that becomes the new interface of the resource, and the inner interface `in` that is connected to the interface of the existing resource. Attaching a converter $\pi$ to a specific interface of a resource $\mathsf{R}$ yields another resource. We understand the left and the right side of the symbol $\mathsf{R}$ as the interface `A` and `E`, respectively; thus, attaching $\pi$ at interface `A` is denoted $\pi\mathsf{R}$ and attaching it at interface `E` is denoted $\mathsf{R}\pi$. Let $\Sigma$

denote the set of converters. Two converters $\phi$ and $\psi$ can be composed sequentially and in parallel: sequential composition is denoted as $\phi \circ \psi$ such that $(\phi \circ \psi)\mathsf{R} = \phi(\psi\mathsf{R})$ and parallel composition as $[\phi, \psi]$, where $[\phi, \psi][\mathsf{R}, \mathsf{S}] = [\phi\mathsf{R}, \psi\mathsf{S}]$. Moreover, we assume the existence of an identity converter $\mathsf{id}$ such that $\mathsf{id}\mathsf{R} = \mathsf{R}\,\mathsf{id} = \mathsf{R}$.

**Conventions for Describing Systems and Algorithms.** We describe our systems using pseudocode. The following conventions are used: We write $x \leftarrow y$ for assigning the value $y$ to the variable $x$. For a finite set $\mathcal{X}$, $x \xleftarrow{\$} \mathcal{X}$ denotes assigning $x$ uniformly at random a value in $\mathcal{X}$. Furthermore, $x \xleftarrow{\mathsf{P}_X} \mathcal{X}$ denotes sampling $x$ according to the indicated probability distribution $\mathsf{P}_X$ over $\mathcal{X}$.

Queries (also called inputs) to systems consist of a list of arguments, of which the first one is a suggestive keyword. If the input consists only of the keyword we omit the parenthesis, i.e., we write `retrieve` or (`hash, x`). When specifying the domain of the inputs, we ignore the keyword and write (`hash, x`) $\in \mathcal{X}$ to indicate $x \in \mathcal{X}$. If a system outputs a value $x$ at the interface named `int`, we denote this "**output** $x$ at `int`". We generally assume that all resources reply at the same interfaces they have been queried before processing any additional queries. Therefore, if a converter outputs a query at its inside interface, we write "let *var* denote the result" meaning that we wait for the value returned from the connected system and then store it in the variable *var*.

## 2.3 Indifferentiability

In contrast to game-based security definitions, indifferentiability gives composable security guarantees, i.e., the security guarantees obtained are not only with respect to specific attack scenarios but with respect to all possible attacks. The fundamental idea of composition is then to prove the construction of $\mathsf{S}$ from $\mathsf{R}$ in isolation and be assured that in any higher level protocol $\phi$ making use of $\mathsf{S}$, the resource $\mathsf{S}$ can be replaced with $\mathsf{R}$ with the protocol applied, without degrading the security of $\phi$. The system $\mathsf{S}$, while not existing in the real world, therefore serves as an abstraction boundary for the design of cryptographic schemes.

Indifferentiability formalizes this by demanding that there exists an efficient simulator $\sigma$, such that the real setting $\pi\mathsf{R}$ and the ideal setting $\mathsf{S}\sigma$ are indistinguishable according to the following definitions.

**Definition 2.1.** The advantage of $D$ in distinguishing $\mathsf{R}$ and $\mathsf{S}$ is defined as

$$\Delta^{\mathsf{D}}(\mathsf{R}, \mathsf{S}) := \Pr[\mathsf{DS} = 1] - \Pr[\mathsf{DR} = 1],$$

where $\mathsf{DS}$ denotes the output of the distinguisher $\mathsf{D}$ when connected to the resource $\mathsf{S}$. The distinguisher thereby gets access to both interfaces of the resource $\mathsf{S}$. Moreover, let $\mathsf{R} \approx \mathsf{S}$ denote that $\Delta^{\mathsf{D}}(\mathsf{R}, \mathsf{S})$ is negligible for every efficient $\mathsf{D}$.

**Definition 2.2** (Indifferentiability)**.** Let $\mathsf{R}$ and $\mathsf{S}$ be 2-interface resources. $\mathsf{S}$ is reducible to $\mathsf{R}$ by $\pi \in \Sigma$ in the sense of indifferentiability (denoted $\mathsf{R} \overset{\pi}{\Longmapsto} \mathsf{S}$), if

$$\mathsf{R} \overset{\pi}{\Longmapsto} \mathsf{S} \quad :\Longleftrightarrow \quad \exists \sigma \in \Sigma : \pi\mathsf{R} \approx \mathsf{S}\sigma,$$

where we refer to $\pi$ and $\sigma$ as the protocol and the simulator, respectively.


Figure 2: The real (left) and the ideal (right) setting considered in indifferentiability. We depict resources using rectangular boxes and converters using rounded boxes. The honest party's interface is depicted on the left, and the dishonest's on the right side.

The formalism of indifferentiability composes in the natural way under some standard closure assumptions[1] on the sets $\Sigma$ and $\mathcal{D}$ of converters and distinguishers considered. First, if $\mathsf{T}$ is reducible to $\mathsf{S}$ and $\mathsf{S}$ is reducible to $\mathsf{R}$, then $\mathsf{T}$ is reducible to $\mathsf{R}$ by the composed protocol. Secondly, if $\mathsf{S}$ is reducible to $\mathsf{R}$, then for any resource $\mathsf{U}$, $[\mathsf{S},\mathsf{U}]$ is reducible to $[\mathsf{R},\mathsf{U}]$. More formally, for any resources $\mathsf{R}$, $\mathsf{S}$, $\mathsf{T}$, and $\mathsf{U}$ we have the following two conditions:

$$\mathsf{R} \overset{\pi_1}{\Longrightarrow} \mathsf{S} \wedge \mathsf{S} \overset{\pi_2}{\Longrightarrow} \mathsf{T} \implies \mathsf{R} \overset{\pi_2 \circ \pi_1}{\Longrightarrow} \mathsf{T}$$

$$\mathsf{R} \overset{\pi}{\Longrightarrow} \mathsf{S} \implies [\mathsf{R},\mathsf{U}] \overset{[\pi,\mathsf{id}]}{\Longrightarrow} [\mathsf{S},\mathsf{U}].$$

# 3 Context-Restricted Indifferentiability

In this section we first revisit the motivation behind composable frameworks such as the indifferentiability framework. To handle cases where fully composable security is unachievable, we then introduce the notion of context-restricted indifferentiability, a single-stage security definition inspired by the original motivation behind the UCE-framework. In fact, in the next section we then prove that UCE can be seen as a special case of context-restricted indifferentiability.

## 3.1 The Limitations of General Composability

At the heart of every composable cryptographic framework, such as indifferentiability, lies the concept of a resource (called functionality in the UC framework). A resource $\mathsf{S}$ captures the idea of a module which provides some well-defined functionality to the different parties–both the honest and the dishonest ones–which can then be used in a higher level protocol. The goal of a protocol $\pi$ is then phrased as constructing the resource $\mathsf{S}$ from an assumed resource $\mathsf{R}$ and the fundamental idea of composition is to prove the construction of $\mathsf{S}$ from $\mathsf{R}$ in isolation and be assured that in any environment, the resource $\mathsf{S}$ can be replaced with $\pi\mathsf{R}$, without degrading the security. This allows for a modular approach, since the construction of the resource $\mathsf{S}$ can be considered entirely independent of its use.

The modular approach of indifferentiability, however, fails if we use a resource $\mathsf{S}$ which cannot be reduced to any $\mathsf{R}$ available in the physical world, such as the random oracle. Let $\mathsf{PO}$ denote a public random oracle resource, and $\mathsf{HK}$ a public hash key resource. Then, the famous impossibility result [CGH04] implies, that there exists no deterministic and stateless protocol $\mathsf{h}$, implementing a hash function, such that $\mathsf{HK} \overset{\mathsf{h}}{\Longrightarrow} \mathsf{PO}$, i.e., such that the hash function reduces the random oracle to the public hash key.

[1] The set of distinguishers $\mathcal{D}$ needs to be closed under emulation of a resource and converter. The set of converters needs to be closed under sequential composition and parallel composition with the identity converter.


Figure 3: The real (left) and the ideal (right) setting considered in context-restricted indifferentiability for a specific context $(\mathsf{f}, \mathsf{P})$ consisting of the filter $\mathsf{f}$ and the auxiliary parallel resource $\mathsf{P}$.

Traditionally, such an impossibility result is circumvented by weakening the guarantees $\mathsf{S}$, and instead consider a restricted variant $\mathsf{S}'$. However, for the random oracle, and many other examples, no such natural weakened version exists. As a second approach, one can restrict the class of distinguishers allowed. The UCE framework is such an approach. Unless there is an application scenario where one can justify such a restricted attacker, this approach leads, however, to security definitions without evident semantics. The original motivation of the UCE framework, though, has not been to consider restricted adversaries but to phrase that, in contrast to the impossibility results, real-world protocols use the random oracle in "sensible" ways. In the following, we turn this motivation into a third approach: We restrict composition in a well-defined way. If there is a resource $\mathsf{S}$ that cannot be reduced to a resource $\mathsf{R}$ in all contexts, we propose to make explicit in which contexts one *can* do it.

### 3.2 Context-Restriction

In this section we formally define the idea of restricting composition. In order to do so, we define a context in which we allow the resource $\mathsf{S}$ to be used. A context consists of an auxiliary parallel resource $\mathsf{P}$ and some converter $\mathsf{f}$ applied by the honest party. We usually call this converter $\mathsf{f}$ a *filter* to indicate that its goal is to restrict the access to the resource $\mathsf{S}$. To obtain general statements, we consider a *set* of contexts instead of a single one. This set should be general enough to capture many application scenarios but avoid those for which the impossibility is known.

**Definition 3.1.** A context set $\mathcal{C}$ is a subset of $\Sigma \times \Phi$, where $\Sigma$ denotes the set of all converters and $\Phi$ denotes the set of all resources.

Recall that our goal is to make a modular statement: reducing $\mathsf{S}$ to another resource $\mathsf{R}$ in each of these contexts in $\mathcal{C}$, i.e., finding a single resource $\mathsf{R}$ and protocol $\pi$ such that $\pi\mathsf{R}$ can instantiate $\mathsf{S}$ in each of these contexts in $\mathcal{C}$. Therefore, the same context appears in both the real and the ideal setting. See Figure 3 for an illustration of the distinction problem when fixing a specific context. Quantifying over all contexts of a set leads to the following definition of *context-restricted indifferentiability*.

**Definition 3.2.** Let $\mathcal{C} \subseteq \Sigma \times \Phi$ be a given set of contexts, and let $\mathsf{R}$ and $\mathsf{S}$ be 2-interface resources. We define $\mathsf{S}$ to be $\mathcal{C}$-restricted reducible to $\mathsf{R}$ by $\pi \in \Sigma$ in the sense of indifferentiability (denoted $\mathsf{R} \overset{\pi,\mathcal{C}}{\underset{\mathsf{cr}}{\Longrightarrow}} \mathsf{S}$), as

$$\mathsf{R} \overset{\pi,\mathcal{C}}{\underset{\mathsf{cr}}{\Longrightarrow}} \mathsf{S} \quad :\Longleftrightarrow \quad \forall(\mathsf{f},\mathsf{P}) \in \mathcal{C}\ \exists\sigma \in \Sigma\colon\ \mathsf{f}[\pi\mathsf{R},\mathsf{P}] \approx \mathsf{f}[\mathsf{S},\mathsf{P}]\sigma$$

and refer to the converters $\pi$ and $\sigma$ as the protocol and the simulator, respectively.

### 3.3 Composition

Composability generally refers to the property of a framework that from one, or multiple, given statements, new ones can be automatically deduced in a sound way without having to reprove them. More concretely, in CRI we are interested in deducing new reducibility statements from given ones. Using the abstract algebraic approach of constructive cryptography [MR11; Mau11], such composition properties are usually consequences of composition-order invariance, a natural associativity property stating that the order in which we connect systems is irrelevant.

Before stating the composition theorem, we first observe that when a resource $\mathsf{S}$ is reduced to $\mathsf{R}$ in a context $(\mathsf{f}, \mathsf{P})$, the overall environment of $\mathsf{S}$ actually consists of both $(\mathsf{f}, \mathsf{P})$ and the distinguisher. Especially, if $\mathsf{S}$ can be reduced to $\mathsf{R}$ within $(\mathsf{f}, \mathsf{P})$, so can it within $(\mathsf{f}' \circ \mathsf{f}, [\mathsf{P}, \mathsf{P}'])$, as $\mathsf{f}'$ and $\mathsf{P}'$ can be absorbed into the distinguisher. This leads to the following closure operation on context sets.

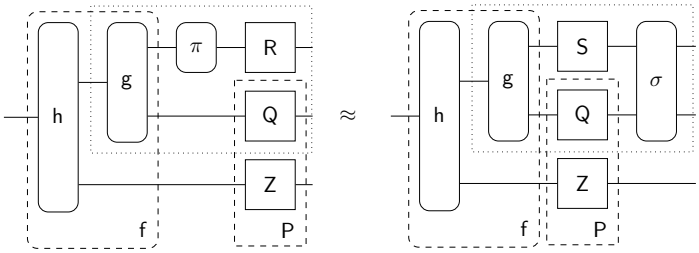
**Definition 3.3.** Let $\mathcal{C} \subseteq \Sigma \times \Phi$ be a given set of contexts. We denote by $\bar{\mathcal{C}} \subseteq \Sigma \times \Phi$ the following set of contexts:

$$\bar{\mathcal{C}} := \{(\mathsf{f}, \mathsf{P}) \in \Sigma \times \Phi \mid \exists (\mathsf{g}, \mathsf{Q}) \in \mathcal{C}\ \exists \mathsf{h} \in \Sigma\ \exists \mathsf{U} \in \Phi :\ \mathsf{h} \circ \mathsf{g} = \mathsf{f} \ \wedge\ [\mathsf{Q}, \mathsf{U}] = \mathsf{P}\}.$$

The following proposition states the context-restricted indifferentiability is idempotent under the closure of the context set.

**Proposition 3.4.** *Let* $\mathsf{R}, \mathsf{S} \in \Phi$ *denote resources,* $\pi \in \Sigma$ *denote a converter, and let* $\mathcal{C}$ *denote a set of contexts. We then have* $\mathsf{R} \overset{\pi,\mathcal{C}}{\underset{\mathsf{cr}}{\Longrightarrow}} \mathsf{S} \iff \mathsf{R} \overset{\pi,\bar{\mathcal{C}}}{\underset{\mathsf{cr}}{\Longrightarrow}} \mathsf{S}$.

*Proof.* The implication $\Longleftarrow$ is trivial, since $\mathcal{C} \subseteq \bar{\mathcal{C}}$. We now prove the other direction. Let $(\mathsf{f}, \mathsf{P}) \in \bar{\mathcal{C}}$ and notice that by Definition 3.3 this implies that there exists $(\mathsf{g}, \mathsf{Q}) \in \mathcal{C}$, $\mathsf{h} \in \Sigma$, and $\mathsf{Z} \in \Phi$ such that $\mathsf{h} \circ [\mathsf{g}, \mathsf{id}] = \mathsf{f}$ and $[\mathsf{Q}, \mathsf{Z}] = \mathsf{P}$.




By our assumption, we know that $\mathsf{g}[\pi, \mathsf{id}][\mathsf{R}, \mathsf{Q}]$ is indistinguishable from $\mathsf{g}[\mathsf{S}, \mathsf{Q}]\sigma$, as indicated by the dotted box. Thus, if we add the additional filter $\mathsf{h}$ and resource $\mathsf{Z}$, they remain indistinguishable. This concludes the proof. □

We now state the formal composition theorem of context-restricted indifferentiability. Note that the additional conditions compared to the composition theorem of classical indifferentiability (cf. Section 2.3) are a direct consequence of the context restrictions. For instance, if in the sequential case we reduce $\mathsf{T}$ to $\mathsf{S}$ in one of the given contexts, we have to ensure that now we are again in a valid context for reducing $\mathsf{S}$ to $\mathsf{R}$. This highlights that in order for context-restricted indifferentiability to be useful, the context sets have to be defined in a form that containment can be easily verified.

**Theorem 3.5.** *Let* $\mathsf{R}$, $\mathsf{S}$, $\mathsf{T}$, *and* $\mathsf{U}$ *denote resources, let* $\pi_1$ *and* $\pi_2$ *denote protocols, and* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *contexts sets. We have*

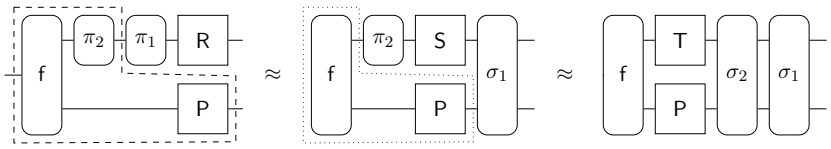
$$\mathsf{R} \overset{\pi_1,\mathcal{C}_1}{\underset{\mathsf{cr}}{\Longrightarrow}} \mathsf{S} \ \wedge\ \mathsf{S} \overset{\pi_2,\mathcal{C}_2}{\underset{\mathsf{cr}}{\Longrightarrow}} \mathsf{T} \quad \Longrightarrow \quad \mathsf{R} \overset{\pi_2 \circ \pi_1,\mathcal{C}_2}{\underset{\mathsf{cr}}{\Longrightarrow}} \mathsf{T},$$

*iff for all* $(\mathsf{f},\mathsf{P}) \in \mathcal{C}_2$ *it holds that* $(\mathsf{f} \circ [\pi_2, \mathsf{id}], \mathsf{P}) \in \overline{\mathcal{C}_1}$. *Moreover, we have*

$$\mathsf{R} \overset{\pi_1,\mathcal{C}_1}{\underset{\mathsf{cr}}{\Longrightarrow}} \mathsf{S} \quad \Longrightarrow \quad [\mathsf{R},\mathsf{U}] \overset{\pi_1,\mathcal{C}_2}{\underset{\mathsf{cr}}{\Longrightarrow}} [\mathsf{S},\mathsf{U}],$$

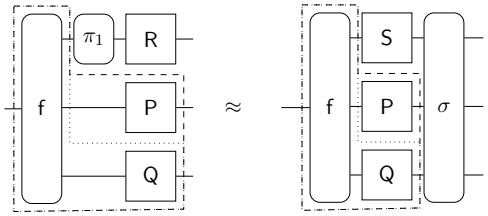
*iff for all* $(\mathsf{f},\mathsf{P}) \in \mathcal{C}_2$ *it holds that* $(\mathsf{f}, [\mathsf{U},\mathsf{P}]) \in \overline{\mathcal{C}_1}$.

*Proof.* We first show the sequential case. Assume that the prerequisite regarding the two context sets is satisfied. Moreover, consider an arbitrary context $(\mathsf{f},\mathsf{P}) \in \mathcal{C}_2$ and the three system configurations, depicted in the following figure.




Using the assumed property on $\mathcal{C}_1$ and Proposition 3.4, we know that the context indicated with the dashed line is a valid one for reducing $\mathsf{S}$ to $\mathsf{R}$, yielding the first equality. The second equality follows directly from the premise.

In order to show the parallel composition property, assume again that the corresponding condition on the context sets is satisfied. Moreover, consider an arbitrary context $(\mathsf{f},\mathsf{P}) \in \mathcal{C}_1$ and the two system configurations, depicted in the following figure.




Using the assumed property on $\mathcal{C}_1$ and Proposition 3.4, we know that the context indicated with the dashed line is a valid one for reducing $\mathsf{S}$ to $\mathsf{R}$. In short, parallel composition in CRI is just associativity: The resource $\mathsf{Q}$ can be seen as both part of the context, indicated by the dashed line, or part of the real and ideal resources, indicated by the dotted line. This concludes the overall proof. □

### 3.4 Relation to Indifferentiability

Let $\mathsf{id}$ denote the identity converter, such that $\mathsf{id}\mathsf{R} = \mathsf{R}$ and $\square$ the neutral resource, such that $[\mathsf{R},\square] = \mathsf{R}$, for any resource $\mathsf{R}$. It is then easy to see that regular indifferentiability, which guarantees full composition, is a special case of context-restricted indifferentiability with the context set $\mathcal{C}_{\mathrm{id}} \coloneqq \{(\mathsf{id},\square)\}$, since $\overline{\mathcal{C}_{\mathrm{id}}} = \Sigma \times \Phi$, i.e., the closure equals to the set of all resources and converters. One can, however, also take the opposite point of view and consider context-restricted indifferentiability to be a special case of plain indifferentiability. From this perspective, CRI reducibility is just a set of normal reducibility statements where the context is part of the considered resources and protocols, respectively. This can be summarized in the following proposition.

**Proposition 3.6.** *Let* $\mathcal{C}_{\mathrm{id}} \coloneqq \{(\mathsf{id},\square)\}$. *For all resources* $\mathsf{R}$, $\mathsf{S}$, *protocol* $\pi$, *and context*

*sets* $\mathcal{C} \subseteq \Sigma \times \Phi$*, we have*

$$\mathsf{R} \overset{\pi}{\Longrightarrow} \mathsf{S} \iff \mathsf{R} \underset{\mathsf{cr}}{\overset{\pi,\mathcal{C}_{\mathrm{id}}}{\Longrightarrow}} \mathsf{S},$$

$$\mathsf{R} \underset{\mathsf{cr}}{\overset{\pi,\mathcal{C}}{\Longrightarrow}} \mathsf{S} \iff \forall(\mathsf{f},\mathsf{P}) \in \mathcal{C}\colon\ [\mathsf{R},\mathsf{P}] \overset{\mathsf{f}\circ[\pi,\mathsf{id}]}{\Longrightarrow} \mathsf{f}[\mathsf{S},\mathsf{P}].$$

*Proof.* This follows directly from Definitions 2.2 and 3.2, and the definitions of the identity converter $\mathsf{id}$ and the neutral resource $\square$. $\square$

Using $\overline{\mathcal{C}_{\mathrm{id}}} = \Sigma \times \Phi$, it is also easy to see that the composition theorem of regular indifferentiability is just a special case of Theorem 3.5.

### 3.5 An Example of CRI: Diffie-Hellman Key Exchange

**The general setting.** Consider the following simple example: two honest parties, e.g., Alice and Bob, perform a Diffie-Hellman key exchange using authenticated communication and then extract an actual key by hashing the group element $g^{ab}$, while an eavesdropper is present.

Since both the honest parties hash the exactly same element, there is no necessity to treat them as different parties and we can work in the indifferentiability setting with one honest party and the adversary. Consider the following resources: let $\mathsf{DH}$ be a Diffie-Hellman resource (modeling the authenticated key exchange) that outputs $g^{ab}$ at interface $\mathtt{A}$ and $(g^a, g^b)$ at interface $\mathtt{E}$, let $\mathsf{PO}$ denote a random oracle accessible by both parties, let $\mathsf{HK}$ denote a public hash key resource that outputs the key at both interfaces, and let $\mathsf{KEY}$ be a resource that outputs a uniformly random key at interface $\mathtt{A}$ and nothing at interface $\mathtt{E}$. The Diffie-Hellman converter $\pi$ takes the group element $g^{ab}$ at the inside interface, inputs it to the random oracle, and outputs the obtained result at the outside interface. It is easy to see that under the CDH assumption we have $[\mathsf{PO},\mathsf{DH}] \overset{\pi}{\Longrightarrow} \mathsf{KEY}$, using the simulator $\sigma$ that chooses $(g^a, g^b)$ uniformly at random and simulates the interface $\mathtt{E}$ of the public random oracle. Note that the fact that the random oracle "vanishes" and is simulated in the ideal world corresponds to the notion of a programmable random oracle...

**Limitation of Indifferentiability.** The explicit appearance of the resource $\mathsf{PO}$ in the above statement corresponds to a proof in the so called random oracle model. The corresponding simulator $\sigma$ chooses $(g^a, g^b)$ uniformly at random and simulates the interface $\mathtt{E}$ of the public random oracle[2]. If we want to obtain a proof in the standard model, i.e., getting rid of the assumed random oracle resource, we would need to find a (potentially) keyed hash function that instantiates the random oracle, which is of course impossible. Such a hash function is in our terminology just a converter $\mathsf{h}$ that reduces the random oracle to the public hash key resource $\mathsf{HK}$, i.e., $\mathsf{HK} \overset{\mathsf{h}}{\Longrightarrow} \mathsf{PO}$. If we had such a hash function, we could use parallel composition to obtain $[\mathsf{HK},\mathsf{DH}] \overset{[\mathsf{h},\mathsf{id}]}{\Longrightarrow} [\mathsf{PO},\mathsf{DH}]$ and then sequential composition to obtain $[\mathsf{HK},\mathsf{DH}] \overset{\pi\circ[\mathsf{h},\mathsf{id}]}{\Longrightarrow} \mathsf{KEY}$.

[2]The fact that the random oracle "vanishes" and is simulated in the ideal world corresponds to the notion of a programmable random oracle.

**Applying CRI.** The main obstacle in the way of the modular approach is that there exists no hash function that reduces the random oracle to a public hash key. However, using the formalism of context-restricted indifferentiability there might be a context set $\mathcal{C}$ such that the random oracle is reducible for a given hash function $\mathsf{h}$. Composing this with the second step should then be possible as long as the protocol which we want to actually apply is in the context set, i.e., $(\pi, \mathsf{DH}) \in \mathcal{C}$. We now show, that this is exactly what the composition theorem of CRI yields:

Assume that $\mathsf{HK} \overset{\mathsf{h},\mathcal{C}}{\underset{\mathsf{cr}}{\Longrightarrow}} \mathsf{PO}$ for some context set $\mathcal{C}$ with $(\pi, \mathsf{DH}) \in \mathcal{C}$. Let $\mathcal{C}' := \{([\pi, \mathsf{id}], \square)\}$. According to the parallel composition rule of Theorem 3.5, we have that $[\mathsf{HK}, \mathsf{DH}] \overset{\mathsf{h},\mathcal{C}'}{\underset{\mathsf{cr}}{\Longrightarrow}} [\mathsf{PO}, \mathsf{DH}]$, since by definition of the identity converter and the neutral resource, $([\pi, \mathsf{id}], [\mathsf{DH}, \square])$ is equivalent to $(\pi, \mathsf{DH})$ and thus contained in $\mathcal{C}$. Using Proposition 3.4, we moreover have $[\mathsf{PO}, \mathsf{DH}] \overset{\pi,\mathcal{C}_{id}}{\underset{\mathsf{cr}}{\Longrightarrow}} \mathsf{KEY}$ and since by definition $(\mathsf{id} \circ [\pi, \mathsf{id}], \square) = ([\pi, \mathsf{id}], \square) \in \mathcal{C}'$, we can apply sequential composition and obtain $[\mathsf{HK}, \mathsf{DH}] \overset{\pi\circ\mathsf{h},\mathcal{C}_{id}}{\underset{\mathsf{cr}}{\Longrightarrow}} \mathsf{KEY}$, which is equivalent to $[\mathsf{HK}, \mathsf{DH}] \overset{\pi\circ\mathsf{h}}{\Longrightarrow} \mathsf{KEY}$.

In summary, this shows that the composition theorem of context-restricted indifferentiability yields exactly what one expects: composition works if and only if the considered application is in the set of allowed contexts. This of course implies that the context set must be defined in such a way that verifying this fact becomes as easy as possible. For the above example, for instance, it is easy to see that this works if $\mathcal{C}$ is the context-set of split-security combined with computational unpredictability, or statistical unpredictability if we are willing to assume DDH instead of CDH. Split security is discussed in more detail in Section 6.

# 4 Modeling UCE in CRI

In the following section we consider the ROM in context-restricted indifferentiability, i.e., consider the special case of CRI where the ideal-world resource $\mathsf{S}$ that we reduce is a random oracle. We then prove that the UCE framework is actually a special case of CRI with a random oracle.

## 4.1 Applying CRI to the ROM

In the following, let $H\colon H.\mathcal{K} \times H.\mathcal{X} \to H.\mathcal{Y}$ denote a keyed hash function, let $\mathsf{HK}_\mathsf{H}$ denote the public hash-key resource that chooses a key for $H$ and outputs it at both interfaces, let $\mathsf{hash}_\mathsf{H}$ denote the converter that implements an oracle for $H$ at the outside interface when connected to $\mathsf{HK}_\mathsf{H}$ at the inside interface, and let $\mathsf{H} := \mathsf{hash}_\mathsf{H}\mathsf{HK}_\mathsf{H}$ as a shorthand. Finally, let $\mathsf{RO}_\mathsf{H}$ denote the private random oracle resource with the same input and output domains as $H$, where by private we mean that this resource only accepts queries at interface $\mathtt{A}$.[3] See Figure 4 for a formal description of these resources and converters.

We now present an alternative formalization of UCE based on context-restricted indifferentiability, more concretely that every possible UCE-class $\mathcal{S}^x$, where $x \in \{\mathrm{sup}, \mathrm{cup}, \mathrm{srs}, \mathrm{crs}, \mathrm{splt}, \ldots\}$, can be mapped to a set of contexts $\mathcal{C}^x$ for which the UCE statement implies the context-restricted indifferentiability statement $\mathsf{HK}_\mathsf{H} \overset{\mathsf{hash}_\mathsf{H},\mathcal{C}}{\underset{\mathsf{cr}}{\Longrightarrow}} \mathsf{RO}$,

[3] The choice to consider a private random oracle stems from the fact that in the UCE framework the hash key is just chosen uniformly at random instead of allowing an arbitrary efficient simulator with access to the random oracle to generate this key.

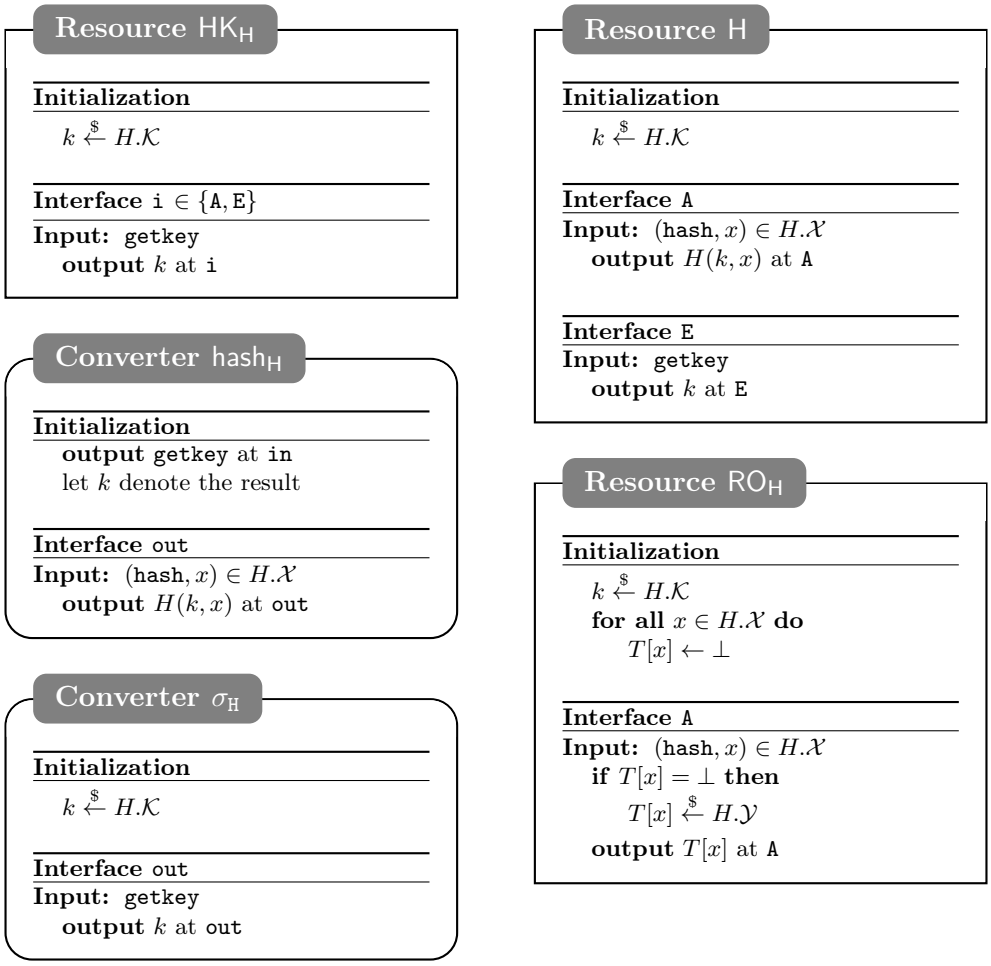



Figure 4: Formal definitions of the resources and converters.

and moreover, if the CRI statement were restricted to a specific simulator, the reverse direction would hold as well.

## 4.2 Non-Interactive Contexts

In order to map every UCE-class to an equivalent set of contexts, we first introduce the set of non-interactive contexts, i.e., the communication between the source and the distinguisher being unidirectional. This restricted set of contexts faithfully encodes the structural restrictions of the traditional UCE game (cf. page 6), where the communication between the source and the distinguisher is unidirectional. Recall that we are in the same general setting as the classical indifferentiability framework, where one only considers out-bound resources for which communication at one interface does not affect the other interface.

**Definition 4.1.** A *non-interactive resource* $\mathsf{P}$ is a resource that at the interface E accepts at most a single trigger query (usually called `retrieve`), and a *non-interactive filter* is a converter that at the outer interface just accepts a single trigger query (usually called `retrieve`). Let $\Phi^{\mathsf{ni}}$ denote the set of all non-interactive resources, and $\Sigma^{\mathsf{ni}}$ denote the set of all non-interactive filters, respectively.

Each UCE-source naturally corresponds to a set of non-interactive contexts. This is formally stated in the following lemma by providing a surjective mapping from the set of non-interactive contexts to the set of UCE sources $\mathcal{S}$.

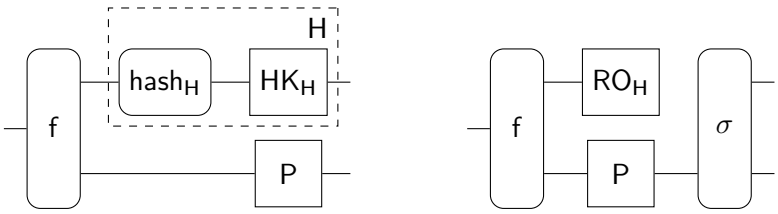



Figure 5: The real (left) and the ideal (right) setting of context-restricted indifferentiability when applied to UCE.

**Lemma 4.2.** *The function* $\phi\colon \Sigma^{\mathsf{ni}} \times \Phi^{\mathsf{ni}} \to \mathcal{S}$ *that maps every context* $(\mathsf{f},\mathsf{P})$ *to the following UCE source* $S$*, that internally emulates* $\mathsf{f}$ *and* $\mathsf{P}$*, is surjective.*

1. *$S$ queries the interface* $\mathtt{E}$ *of* $\mathsf{P}$ *to obtain* $z$*.*
2. *$S$ queries the outside interface of the filter* $\mathsf{f}$ *to obtain* $y$*. The queries at the inside interface of* $\mathsf{f}$ *are forwarded to the resource* $\mathsf{P}$ *or output as queries to the hash oracle, respectively.*
3. *$S$ outputs* $L = (y, z)$*.*

*Proof.* First, it is easy to see that $\phi$ is indeed a function from $\Sigma^{\mathsf{ni}} \times \Phi^{\mathsf{ni}}$ to $\mathcal{S}$, i.e., $\phi(\mathsf{f},\mathsf{P})$ is a valid UCE source for every context $(\mathsf{f},\mathsf{P}) \in \Sigma^{\mathsf{ni}} \times \Phi^{\mathsf{ni}}$. To see that this function is surjective, fix an arbitrary source $S$. Now, let $\mathsf{f}_{\mathsf{S}}$ denote the filter that upon receiving the query `retrieve` at the outer interface internally runs $\mathsf{S}$ and answers this query with the leakage $L$. Each hash query of $\mathsf{S}$ is output at the inner sub-interface `in.H` and the corresponding answer is forwarded to $\mathsf{S}$. Clearly $\phi(\mathsf{f}_{\mathsf{S}}, \square) = S$, where $\square \in \Phi^{\mathsf{ni}}$ denotes the dummy resource. □

### 4.3 ROM-CRI Security Implies UCE Security

We now show, that for the specific simulator $\sigma_{\mathtt{H}}$ that chooses the hash key uniformly at random, the distinguishing problem of context-restricted indifferentiability for a fixed context $(\mathsf{f},\mathsf{P})$ is as hard as the UCE game with the source $\phi(\mathsf{f},\mathsf{P})$. In order to relate more directly to the traditional UCE definition, we first introduce the RO-CRI advantage, which is depicted in Figure 5 for a specific context $(\mathsf{f},\mathsf{P}) \in \mathcal{C}$.

**Definition 4.3.** We define the *random-oracle context-restricted indifferentiability (RO-CRI)* advantage of a distinguisher $\mathsf{D}$ on a hash function $\mathsf{H}$ in a context $(\mathsf{f},\mathsf{P})$ as

$$\mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f},\mathsf{P},\sigma}(\mathsf{D}) \coloneqq \Delta^{\mathsf{D}}(\mathsf{f}[\mathsf{H},\mathsf{P}], \mathsf{f}[\mathsf{RO}_{\mathsf{H}},\mathsf{P}]\sigma),$$

for a simulator $\sigma$. If there exists a simulator $\sigma$ such that for all efficient distinguishers and all contexts $(\mathsf{f},\mathsf{P}) \in \mathcal{C}$, the RO-CRI advantage is negligible, we say that $\mathsf{H}$ is $\mathcal{C}$ random-oracle context-restricted indifferentiable.

The following lemma implies that for non-interactive contexts this definition is equivalent to the game-based definition of UCE-security, if we fix the simulator to $\sigma_{\mathtt{H}}$.

**Lemma 4.4.** *Let* $\mathcal{S}$ *denote the set of all UCE-sources and* $\phi\colon \Sigma^{\mathsf{ni}} \times \Phi^{\mathsf{ni}} \to \mathcal{S}$ *the surjective function from Lemma 4.2. For every distinguisher* $\mathsf{D}$*, there is a distinguisher* $\mathsf{D}'$ *(with essentially the same efficiency) with*

$$\forall (\mathsf{f},\mathsf{P}) \in \Sigma^{\mathsf{ni}} \times \Phi^{\mathsf{ni}}\colon \mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f},\mathsf{P},\sigma_{\mathtt{H}}}(\mathsf{D}) = \mathbf{Adv}^{\text{uce}}_{H,\phi(\mathsf{f},\mathsf{P}),\mathsf{D}'},$$

*where* $\mathbf{Adv}^{\text{uce}}_{H,S,D}$ *denotes the uce-advantage of* $(S, D)$ *on* $H$*. Conversely, for every distinguisher* $\mathsf{D}'$ *there is an equally efficient distinguisher* $\mathsf{D}$ *such that for all* $(\mathsf{f}, \mathsf{P}) \in \Sigma^{\mathsf{ni}} \times \Phi^{\mathsf{ni}}$ *we have* $\mathbf{Adv}^{\text{uce}}_{H,\phi(\mathsf{f},\mathsf{P}),\mathsf{D}'} = \mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f},\mathsf{P},\sigma_{\mathtt{H}}}(\mathsf{D})$.

*Proof.* For every distinguisher $\mathsf{D}$ for $\mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f},\mathsf{P},\sigma_{\mathtt{H}}}(\mathsf{D})$ we can construct a distinguisher $\mathsf{D}'$ using a wrapper around $\mathsf{D}$ as follows: if $\mathsf{D}$ queries the interface $\mathtt{E}$ of the hash resource (for the key) or $\mathsf{P}$ we return $hk$ or $z$, respectively; if $\mathsf{D}$ queries the outer interface of $\mathsf{f}$, then $y$ is returned. The bit $b'$ is then set to the output bit of $\mathsf{D}$. The key observation is that the resources $\mathsf{f}[\mathsf{H}, \mathsf{P}]$ and $\mathsf{f}[\mathsf{RO}, \mathsf{P}]\sigma_{\mathtt{H}}$ are independent to the order in which $\mathsf{D}$ does those queries. It is now easy to see that $\mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f},\mathsf{P},\sigma_{\mathtt{H}}}(\mathsf{D}) = \mathbf{Adv}^{\text{uce}}_{H,\phi(\mathsf{f},\mathsf{P}),\mathsf{D}'}$.

The reverse direction works with an analogous wrapper that first queries the system to obtain $hk$, $z$, and $y$. It then invokes $\mathsf{D}'$ with $hk$ and $L = (y, z)$ as inputs and outputs the bit $b'$. □

We now state the main result of this section, relating the UCE game to context-restricted indifferentiability. It implies that instead of viewing the source as the first stage of an adversary, one can view it as the set of contexts in which the hash function can safely be used.

**Theorem 4.5.** *Let* $\mathcal{D}$ *denote the set of all efficient distinguishers. For every class* $\mathcal{S}^x$ *of UCE sources, there exists a set of contexts* $\mathcal{C}^x$ *such that* $\mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f},\mathsf{P},\sigma_{\mathtt{H}}}(\mathsf{D})$ *is negligible for every* $D \in \mathcal{D}$ *and every context* $(\mathsf{f}, \mathsf{P}) \in \mathcal{C}^x$ *if and only if* $\mathbf{Adv}^{\text{uce}}_{H,S,D}(\cdot)$ *is negligible for all* $(S, D) \in \mathcal{S}^x \times \mathcal{D}$*.*

*Proof.* Using the surjectivity of $\phi$ (Lemma 4.2), we have that for any UCE-class $\mathcal{S}^x$ we can define $\mathcal{C}^x \coloneqq \phi^{-1}(\mathcal{S}^x)$ such that $\phi(\mathcal{C}^x) = \mathcal{S}^x$. Hence, by Lemma 4.4 we have that $\mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f},\mathsf{P},\sigma_{\mathtt{H}}}(\mathsf{D})$ is negligible for all efficient distinguishers $\mathsf{D} \in \mathcal{D}$ and all contexts $(\mathsf{f}, \mathsf{P}) \in \mathcal{C}^x$ iff $\mathbf{Adv}^{\text{uce}}_{H,S,D}(\cdot)$ is negligible for all $(S, D) \in \mathcal{S}^x \times \mathcal{D}$. □

The following corollary establishes the unidirectional implication from UCE-security to context-restricted indifferentiability. The reverse direction does not necessarily hold, since the context-restricted indifferentiability notion allows for different simulators than the natural one $\sigma_{\mathtt{H}}$.

**Corollary 4.6.** *Let* $\mathcal{D}$ *denote the set of all efficient distinguishers. For every class* $\mathcal{S}^x$ *of UCE sources, there exists a set of contexts* $\mathcal{C}^x$ *such that if* $\mathbf{Adv}^{\text{uce}}_{H,S,D}(\cdot)$ *is negligible for all* $(S, D) \in \mathcal{S}^x \times \mathcal{D}$*, then* $\mathsf{HK}_{\mathsf{H}} \overset{\mathsf{hash}_{\mathsf{H}},\mathcal{C}^x}{\underset{\mathsf{cr}}{\Longrightarrow}} \mathsf{RO}_{\mathsf{H}}$.

*Proof.* This follows directly from Definitions 3.2 and 4.3 and Theorem 4.5. □

## 5 Modeling Public-Seed Pseudorandom Permutations in CRI

In [ST17] Soni and Tessaro introduce the notion of public-seed pseudorandom permutations (psPRP) that are inspired by UCE. In fact, they introduce a generalization of UCE, called public-seed pseudorandomness (psPR), of which both psPRP and UCE are instantiations. In the following, we give an analogous equivalence result to the one of Section 4 between context-restricted indifferentiability and the general public-seed pseudorandomness notion. The equivalence for the psPRP notion then just follows as a trivial corollary.

**Algorithm 13** The public-seed pseudorandomness game (single-session)

**function** MAIN $\text{psPR}^{S,D}_{\text{F},I}(\lambda)$
- $b \xleftarrow{\$} \{0,1\}$
- $k \xleftarrow{\$} \text{F.Kg}(1^\lambda)$
- $f \xleftarrow{\$} I_\lambda$
- $L \xleftarrow{\$} S^{\mathcal{O}}(1^\lambda)$
- $b' \xleftarrow{\$} D(1^\lambda, k, L)$
- **return** $(b' = b)$

**function** $\mathcal{O}(x)$
- **if** $b = 1$ **then**
  - **return** $\text{F.Eval}(1^\lambda, k, x)$
- **else**
  - **return** $f(x)$

Figure 6: The public-seed pseudorandomness security game for a function family F, an ideal primitive $I$, a source $S$, and a distinguisher $D$.

### 5.1 Public-Seed Pseudorandomness

We first briefly recap the main definitions of public-seed pseudorandomness as introduced in [ST17]. The authors first introduce the notion of an ideal primitive, of which both random oracles and ideal random permutations are instantiations of.

**Definition 5.1.** An ideal primitive is a pair $I = (\Sigma, D)$, where $\Sigma = \{\Sigma_\lambda\}_{\lambda\in\mathbb{N}}$ is a family of sets of functions (such that all functions have the same domain and range), and $D = \{D_\lambda\}_{\lambda\in\mathbb{N}}$is a family of probability distributions, where the range of $D_\lambda$ is a subset of $\Sigma_\lambda$ for all $\lambda \in \mathbb{N}$. The ideal primitive $I$, once the security parameter $\lambda$ is fixed, should be thought of as an oracle that initially samples a function $I$ as its initial state according to $D_\lambda$ from $\Sigma_\lambda$. Then, I provides access to $I$ via queries i.e. on input $x$ it returns $I(x)$.

Moreover, the authors of [ST17] then define the following notion of $\Sigma$-compatible function families. A function family corresponds to an algorithm that generalizes hash functions and pseudo-random permutations.

**Definition 5.2.** A function family $\text{F} = (\text{Kg}, \text{Eval})$ consists of a key (or seed) generation algorithm F.Kg and an evaluation algorithm F.Eval.

- F.Kg is a randomized algorithm that on input the unary representation of the security parameter $\lambda$ returns a key $k$, and we let $[\text{F.Kg}(1^\lambda)]$ denote the set of all possible outputs of $\text{F.Kg}(1^\lambda)$.
- F.Eval is a deterministic algorithm that takes three inputs; the security parameter in unary form $1^\lambda$, a key $k \in [\text{F.Kg}(1^\lambda)]$ and a query $x$ such that $\text{F.Eval}(1^\lambda, k, \cdot)$ implements a function that maps queries $x$ to $\text{F.Eval}(1^\lambda, k, x)$.

We say that F is efficient if both Kg and Eval are polynomial-time algorithms.

The goal of such a function family F is then to implement an ideal primitive $I$ with respect to the UCE-like security game depicted in Figure 6, considering an adversary that is split into a source $S$ and a distinguisher $D$. In contrast to the original definition, we only consider the game for a single session, which can easily be related to the multi-session one using a standard hybrid argument.

Finally, Soni and Tessaro define the pspr-advantage as follows:

$$\mathbf{Adv}^{\mathsf{pspr}[I]}_{\text{F},S,D}(\lambda) = 2\Pr\left[\mathsf{psPRS}^{S,D}_{\text{F},I}(\lambda)\right] - 1.$$

## 5.2 Ideal Primitives and Function Families in CRI

In the following section, we argue that every ideal primitive $I$ can be understood as an ideal resource of an CRI statement, and every function family F as an pair of real resource and protocol, respectively. For simplicity, we ignore the security parameter $\lambda$ in the following.

For every ideal primitive $I$ and for every function family $\mathrm{F} = (\mathrm{Kg}, \mathrm{Eval})$, denote the corresponding resource and converters depicted in Figure 7. Moreover, we also define the simulator $\sigma_{\mathtt{F}}$, which simply chooses a key according to Kg as well.

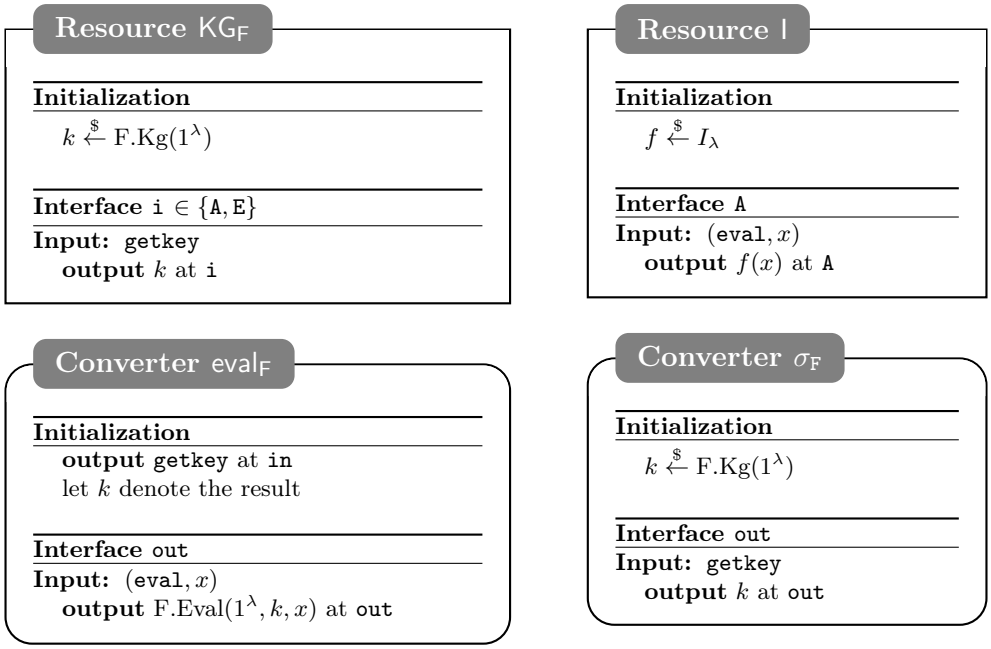



Figure 7: The corresponding resources and converters.

## 5.3 CRI-Security Implies psPR-Security

We now show, that for the specific simulator $\sigma_{\mathtt{KG}}$, if for every specific context $(\mathsf{f}, \mathsf{P})$ the distinguishing problem of context-restricted indifferentiability is hard, then the UCE game with the fixed source $\phi(\mathsf{f}, \mathsf{P})$ is hard as well, and vice versa. In order to relate more directly, we introduce the psRP-CRI advantage.

**Definition 5.3.** We define the *public-seed pseudorandomness context-restricted indifferentiability (psRP-CRI)* advantage of a distinguisher $\mathsf{D}$ on a hash function $\mathsf{H}$ in a context $(\mathsf{f}, \mathsf{P})$ as

$$\mathbf{Adv}^{\mathrm{psPR-CRI}}_{\mathrm{F},\mathsf{I},\mathsf{f},\mathsf{P},\sigma}(\mathsf{D}) \coloneqq \Delta^{\mathsf{D}}(\mathsf{f}[\mathsf{eval}_\mathsf{F}\mathsf{KG}_\mathsf{F}, \mathsf{P}], \mathsf{f}[\mathsf{I}, \mathsf{P}]\sigma),$$

for a simulator $\sigma$.

The following lemma implies that for non-interactive contexts this definition is equivalent to the game-based definition of UCE security, if we fix the simulator to $\sigma_{\mathtt{F}}$.

**Lemma 5.4.** *Let* F *denote a function family and* $I$ *an ideal primitive. Furthermore, let* $\mathcal{S}$ *denote the set of all psPR-sources and* $\phi\colon \Sigma^{\mathsf{ni}} \times \Phi^{\mathsf{ni}} \to \mathcal{S}$ *the surjective function from Lemma 4.2. For every distinguisher* $\mathsf{D}$*, there is a distinguisher* $\mathsf{D}'$ *(with essentially the same efficiency) with*

$$\forall (\mathsf{f}, \mathsf{P}) \in \Sigma^{\mathsf{ni}} \times \Phi^{\mathsf{ni}}\colon \mathbf{Adv}^{\mathrm{psPR-CRI}}_{\mathrm{F},\mathsf{I},\mathsf{f},\mathsf{P},\sigma_\mathrm{F}}(\mathsf{D}) = \mathbf{Adv}^{\mathsf{pspr}[I]}_{\mathrm{F},\phi(\mathsf{f},\mathsf{P}),\mathsf{D}'}$$

*Conversely, for every distinguisher* $\mathsf{D}'$ *there is a distinguisher* $\mathsf{D}$ *(with essentially the same efficiency) such that for all* $(\mathsf{f},\mathsf{P}) \in \Sigma^{\mathsf{ni}} \times \Phi^{\mathsf{ni}}$ *we have* $\mathbf{Adv}^{\mathsf{pspr}[I]}_{\mathrm{F},\phi(\mathsf{f},\mathsf{P}),\mathsf{D}'} = \mathbf{Adv}^{\mathrm{psPR-CRI}}_{\mathrm{F},\mathsf{I},\mathsf{f},\mathsf{P},\sigma_{\mathrm{F}}}(\mathsf{D})$.

*Proof.* The proof is analogous to the one of Lemma 4.4. □

We can now state the main result of this section, relating the public-seed pseudorandomness game to context-restricted indifferentiability.

**Theorem 5.5.** *Let* F *denote a function family,* $I$ *an ideal primitive, and let* $\mathcal{D}$ *denote the set of all efficient distinguishers. For every family* $\mathcal{S}^x$ *of psPR-sources, there exists a set of contexts* $\mathcal{C}^x$ *such that* $\mathbf{Adv}^{\mathrm{psPR-CRI}}_{\mathrm{F},\mathsf{I},\mathsf{f},\mathsf{P},\sigma_{\mathrm{F}}}(\mathsf{D})$ *is negligible for every* $D \in \mathcal{D}$ *and every context* $(\mathsf{f},\mathsf{P}) \in \mathcal{C}^x$ *if and only if* $\mathbf{Adv}^{\mathsf{pspr}[I]}_{\mathrm{F},S,D}(\cdot)$ *is negligible for all* $(S,D) \in \mathcal{S}^x \times \mathcal{D}$.

*Proof.* The proof is analogous to the one of Theorem 4.5. □

This demonstrates that not only UCE is a special case of CRI but also the more general notion of psPR is still a special case of CRI, where each ideal primitive and function family correspond to the ideal and real world, respectively. Similarly to UCE, the psPR notion is still non-interactive and essentially hard-codes a specific simulator in the security game.

## 6 Generalizing Split-Security

In this section, we present generalizations of the split-source UCE-class, that cannot be formalized in plain UCE, based on CRI.

### 6.1 Split-Security

The split-source UCE-class has been proposed by Bellare et al. after it has been shown that computational-unpredictable UCE-security and computational-reset-secure UCE-security is infeasible if indistinguishability obfuscation exists. Note that split-security is not a stand-alone UCE-class in the sense that it is designed to be combined with either computational unpredictability or reset-security, respectively.

The general idea of split-security is, that the source must not be able to compute $\mathrm{Obfs}(H(\cdot, x) = y)$. To achieve this, the source must be dividable into two parts $(S_0, S_1)$, where $S_0$ chooses a vector $(x_1, \ldots, x_n)$ of query points, without having access to the hash oracle, and $S_1$ then just gets the evaluations $y_i := \mathrm{Hash}(x_i)$, without having access to the hash oracle either. Thus, no part of the source knows both $x_i$ and its evaluation $y_i$, preventing the aforementioned iO attack. A formal description of the split-source $S := \mathit{Splt}[S_0, S_1]$ is found in Figure 8.

### 6.2 An Alternative Representation of Split-Security

As established by Theorem 4.5, using $\mathcal{C}^{\mathsf{splt}} := \phi^{-1}(\mathcal{S}^{\mathsf{splt}})$ faithfully translates split-security to CRI. In order to work more easily with split-security and make it more directly comparable to our later generalizations thereof, however, we introduce an alternative representation of the split-security CRI context set using a fixed filter $\mathsf{f}^{\mathsf{splt}}$, which encodes the structural restriction of split-security.

**Algorithm 22** Splt SOURCE

**function** $\textsc{Splt Source}^{\textsc{Hash}}(1^\lambda)$
  $(L_0, x) \xleftarrow{\$} S_0(1^\lambda)$
  **for** $i = 1, \ldots, |x|$ **do**
    $y[i] \leftarrow \textsc{Hash}(x[i])$
  $L_1 \xleftarrow{\$} S_1(1^\lambda, y)$
  $L \leftarrow (L_0, L_1)$
  **output** $L$

Figure 8: The definition of the split-source family in UCE.

**Definition 6.1.** The *split* RO-CRI context set is the set of filters and non-interactive resource pairs of which the filter can be factorized into the filter $\mathsf{f}^{\mathsf{splt}}$, as depicted in Figure 9, followed by an arbitrary filter. Formally,

$$\mathcal{C}^{\mathsf{splt}} := \{\mathsf{f} \circ \mathsf{f}^{\mathsf{splt}} \mid \mathsf{f} \in \Sigma^{\mathsf{ni}}\} \times \Phi^{\mathsf{ni}}.$$

Observe that the filter $\mathsf{f}^{\mathsf{splt}}$ expects the resource $\mathsf{P}$ to output a sequence of pairs $(x_i, a_i)$, where $x_i$ is intended to be unpredictable, then hashes $x_i \parallel a_i$ and outputs the result. Note that the distinction into an unpredictable value $x_i$ and an auxiliary value $a_i$ solely prepares for our generalizations. This type of resource corresponds to the first stage of the source $S_0$ that produces the queries[4] and the leakage $L_0$ (called $Z$ in the following definition), and we will call it a *seed* in the following.

**Definition 6.2.** A *seed with $n$ outputs* is a resource that initially draws random values $X_1, \ldots, X_n$, $A_1, \ldots, A_n$, and $Z$ according to some joint distribution. Then, it accepts at the interface $\mathtt{E}$ a single trigger query (usually called `retrieve`) that is answered with $Z$, and at the interface $\mathtt{A}$ $n$ trigger queries answered with $(X_1, A_1)$ to $(X_n, A_n)$. Let $\Phi_n^{\mathsf{seed}} \subset \Phi^{\mathsf{ni}}$ denote the set of all seeds with $n$ outputs. Moreover, let $\mathcal{C}_n^{\mathsf{seed}} := \Sigma \times \Phi_n^{\mathsf{seed}}$.

The second stage of the source $S_1$ then translates to the additional non-interactive filter $\mathsf{f}$ that gets from $\mathsf{f}^{\mathsf{splt}}$ the hashed values $y_i$ and can further process them to obtain the leakage $L_1$. The following lemma establishes that this represents a correct translation of split-security as well.

**Lemma 6.3.** *Let $\mathcal{S}^{\mathsf{n}}$ denote the class of all UCE sources making at most $n$ oracle queries and let $\phi$ denote the surjective function from Lemma 4.2. We then have*

$$\phi\big(\mathcal{C}^{\mathsf{splt}} \cap \mathcal{C}_n^{\mathsf{seed}}\big) = \mathcal{S}^{\mathsf{splt}} \cap \mathcal{S}^{\mathsf{n}},$$

*and thus, $\mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f},\mathsf{P},\sigma_{\mathtt{H}}}(\mathsf{D})$ is negligible for every $D \in \mathcal{D}$ and every context $(\mathsf{f}, \mathsf{P}) \in \mathcal{C}^{\mathsf{splt}} \cap \mathcal{C}_n^{\mathsf{seed}}$ if and only if $\mathbf{Adv}^{\text{uce}}_{H,S,D}(\cdot)$ is negligible for all $(S, D) \in (\mathcal{S}^{\mathsf{splt}} \cap \mathcal{S}^{\mathsf{n}}) \times \mathcal{D}$.*

*Proof (Sketch).* First, we show that for every $\mathsf{f} \in \Sigma^{\mathsf{ni}}$ and $\mathsf{P} \in \Phi_n^{\mathsf{seed}}$ the context $(\mathsf{f} \circ \mathsf{f}^{\mathsf{splt}}, \mathsf{P})$ is mapped to a UCE source in $\mathcal{S}^{\mathsf{splt}} \cap \mathcal{S}^{\mathsf{n}}$ by $\phi$. To this end, we define $S_0$ to be the source which initially emulates $\mathsf{P}$. It first queries $z$ at the interface $\mathtt{E}$ and all

[4] Here, we only consider split sources with a fixed number of queries. A polynomial number of queries could easily be phrased as well.

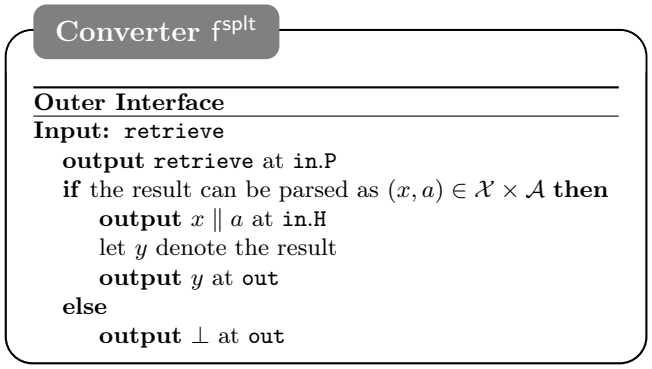



Figure 9: The definition of the filter $\mathsf{f}^{\mathsf{splt}}$. The filter is implicitly parametrized in the two sets $\mathcal{X}$ and $\mathcal{A}$, which should become clear from the context in all of our uses.

values $x = x_1, \ldots, x_n$ at the interface A of P and set $L_0 = z$. The source $S_1$ internally emulates f. It initially queries retrieve towards f to obtain $L_1$. Whenever f outputs a query retrieve towards $\mathsf{f}^{\mathsf{splt}}$, then $S_1$ answers by using the next value $y_i$. Now observe that, by definition of $\Phi^{\mathsf{ni}}$, obtaining all queries $x_1, \ldots, x_n$ from P at interface A on demand or at the beginning and storing the results $y_1 = H(k, x_1), \ldots, y_n = H(k, x_n)$ is equivalent. Thus, it is easy to verify that $\phi(\mathsf{f} \circ \mathsf{f}^{\mathsf{splt}}, \mathsf{P}) = Splt[S_0, S_1]$.

Second, we show that $\phi(\mathcal{C}_n^{\mathsf{splt}}) \supseteq \mathcal{S}^{\mathsf{splt}} \cap \mathcal{S}^{\mathsf{n}}$, i.e., for every split source there exists at least one context that maps to this source. It is easy to see that $S_0$ can be embedded accordingly in a resource $\mathsf{P} \in \Phi_n^{\mathsf{seed}}$ and $S_1$ in a filter $\mathsf{f} \in \Sigma^{\mathsf{ni}}$ such that $\phi(\mathsf{f} \circ \mathsf{f}^{\mathsf{splt}}, \mathsf{P}) = Splt[S_0, S_1]$. The remaining claim about the advantages immediately follows by Lemma 4.4, concluding the proof. □

### 6.3 Strong-Split security

Split sources have several limitations. First, the distinguisher cannot influence the queries at all and, thus, all queries must be solely determined by the honest parties. This prevents, for example, queries like $H(hk, x \| a)$ where $a$ is a value which can be chosen by the distinguisher (e.g. $a$ is transmitted over an insecure channel) even if $x$ is unpredictable. In the following section, we introduce a generalization of split-security, called *strong-split* security, to address this limitation. Second, split-security does not allow nested queries like $H(hk, H(hk, x))$. In Section 6.5 we present a further generalization to address this issue as well.

*Remark.* Note that the first limitation is not specific to split-security, but is inherent to the traditional UCE-game. In their work [FM16] on Interactive Computational Extractors (ICEs), Farshim and Mittelbach have proposed an alternative relaxation of this issue. In Section 6.6 we show that ICE security implies strong-split context-restricted indifferentiability for statistical unpredictability.

In order to allow the distinguisher to influence the queries while ensuring that the overall query is still unpredictable from the viewpoint of the distinguisher, we allow him to apply any *injective* function on the preliminary inputs $x$ specified by the first part of the source $S_0$, which will then be evaluated and passed on to $S_1$. That is, we use the simple fact that for any injective function $f$ guessing $f(x_i)$ is at least as hard as guessing $x_i$. To formally model this as a context set for RO-CRI, we use a specific filter $\mathsf{f}_p^{\mathsf{s-splt}}$. This filter expects the resource P to output a sequence of pairs $(x_i, a_i)$, where $x_i$ is intended to be unpredictable. We will call such

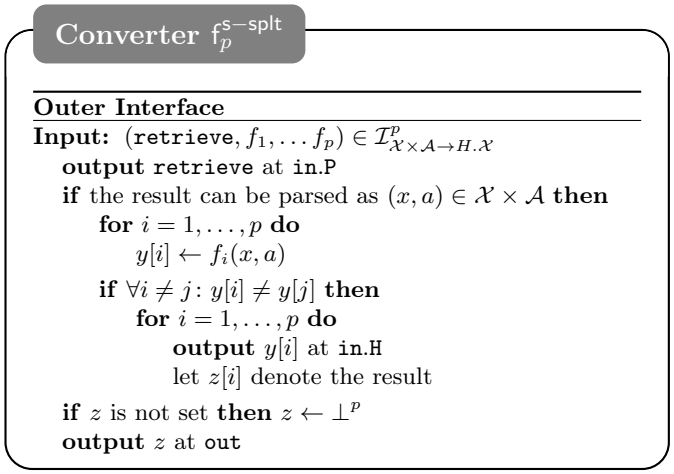



Figure 10: The strong-split filter $\mathsf{f}_p^{\mathsf{s-splt}}$ for RO-CRI, where $\mathcal{I}_{\mathcal{X}\times\mathcal{A}\to H.\mathcal{X}}$ denotes the set of all efficiently computable functions from $\mathcal{X} \times \mathcal{A}$ to $H.\mathcal{X}$ that are injective in the first argument. Note that it was pointed out in [BM14] that the queries of a split-source must be distinct; otherwise arbitrary information can be communicated to the second stage.

a resource $\mathsf{P}$ *seed* in the following. For each of them the distinguisher can then input $p$ functions $f_i^1, \ldots, f_i^p$ that are injective in the first arguments, upon which the filter will output $(f_i^1(x_i, a_i), \ldots, f_i^p(x_i, a_i))$ to the hash oracle and forwards the results to the distinguisher. A formal definition of is depicted in Figure 10. The filter $\mathsf{f}_p^{\mathsf{s-splt}}$ can then be combined with an arbitrary non-interactive resource to obtain a strong-split RO-CRI context.

**Definition 6.4.** The *strong-split* RO-CRI context set is the set of filters and non-interactive resource pairs of which the filter can be factorized into $\mathsf{f}_p^{\mathsf{s-splt}}$ followed by an arbitrary filter. Formally,

$$\mathcal{C}_p^{\mathsf{s-splt}} := \{\mathsf{f} \circ \mathsf{f}_p^{\mathsf{s-splt}} \mid \mathsf{f} \in \Sigma\} \times \Phi^{\mathsf{ni}}.$$

Analogous to split-security, strong-split security is not a sufficient restriction to avoid trivial impossibility results. Rather, these notions are meant to be combined with a notion of unpredictability or reset-security. However, for strong-split security, requiring the seed to output distinct unpredictable values is still insufficient to guarantee the security: for instance, if the resource $\mathsf{P}$ outputs $(x, a_1)$ and $(x + 1, a_2)$, then the distinguisher can easily choose $f$ and $g$ such that $f(x, a_1) = g(x + 1, a_2)$. Therefore, we introduce suitable notion of unpredictability in the next subsection, which when combined with strong-split security presents a plausible assumption for a hash function family.

## 6.4 Strict Min-Entropy Seeds

We now define an information-theoretic restriction on the seed called *strict min-entropy seeds*. Similar to Farshim and Mittelbach [FM16] we choose to focus on statistical rather than computational unpredictability to ensure that our notion excludes interactive version of the attack highlighted in [BFM14].[5] More concretely,

[5]We would like to stress that while split-security was originally introduced for the computational setting, it is still a natural class to consider even when combined with a statistical unpredictability notion.

we consider seeds whose outputs at interface $\mathtt{A}$ consist of pairs $(X_i, A_i)$, with $A_i$ being an auxiliary value, such that $X_i$ has high *average conditional min-entropy* given the leakage $Z$ and all previous queries.

**Definition 6.5.** A *strict min-entropy $k$-bit seed with $n$ outputs* is seed with $n$ outputs (c.f. Definition 6.2), such that

$$\forall i \leq n\colon\ \tilde{H}_\infty\big(X_i \,\big|\, \{X_j\}_{j<i}, \{A_j\}_{j\leq i}, Z\big) \ \geq\ k.$$

Let $\Phi^{\mathsf{s-me}}_{n,k} \subset \Phi^{\mathsf{ni}}$ denote the set of all strict min-entropy $k$-bit seed with $n$ outputs. Moreover, let $\mathcal{C}^{\mathsf{s-me}}_{n,k} \coloneqq \Sigma \times \Phi^{\mathsf{s-me}}_{n,k}$ denote the set of all strict min-entropy $k$-bit contexts.

When combining split-security or strong-split security with strict min-entropy seeds, the security does not depend on the maximal number $n$ of values produced by the seed.

**Lemma 6.6.** *Let $n$ be polynomially bounded. If $H$ is a $\mathcal{C}^{\mathsf{splt}} \cap \mathcal{C}^{\mathsf{s-me}}_{1,k}$ indifferentiable hash function, then $H$ is also $\mathcal{C}^{\mathsf{splt}} \cap \mathcal{C}^{\mathsf{s-me}}_{n,k}$ indifferentiable.*

*More concretely, let $\mathcal{D}$ denote the set of distinguishers. Then there exists $\rho\colon \mathcal{D} \times \left(\mathcal{C}^{\mathsf{splt}} \cap \mathcal{C}^{\mathsf{s-me}}_{n,k}\right) \to \mathcal{D}$ and $\psi\colon \mathcal{C}^{\mathsf{splt}} \cap \mathcal{C}^{\mathsf{s-me}}_{n,k} \to \mathcal{C}^{\mathsf{splt}} \cap \mathcal{C}^{\mathsf{s-me}}_{1,k}$, such that for every $(\mathsf{f},\mathsf{P}) \in \mathcal{C}^{\mathsf{splt}} \cap \mathcal{C}^{\mathsf{s-me}}_{n,k}$ we have*

$$\mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f},\mathsf{P},\sigma}(\mathsf{D}) \leq \binom{n}{2} 2^{-k} + n \cdot \mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f}',\mathsf{X}',\sigma}(\mathsf{D}')$$

*with $\mathsf{D}' \coloneqq \rho(\mathsf{D},\mathsf{f},\mathsf{P})$ and $(\mathsf{f}',\mathsf{X}') \coloneqq \psi(\mathsf{f},\mathsf{P})$.*

*Proof.* The proof is completely analogous to the one of Lemma 6.7. □

**Lemma 6.7.** *Let $n$ be polynomially bounded. If $H$ is a $\mathcal{C}^{\mathsf{s-splt}}_p \cap \mathcal{C}^{\mathsf{s-me}}_{1,k}$ indifferentiable hash function, then $H$ is also $\mathcal{C}^{\mathsf{s-splt}}_p \cap \mathcal{C}^{\mathsf{s-me}}_{n,k}$ indifferentiable.*

*More concretely, let $\mathcal{D}$ denote the set of distinguishers. Then there exists $\rho\colon \mathcal{D} \times \left(\mathcal{C}^{\mathsf{s-splt}}_p \cap \mathcal{C}^{\mathsf{s-me}}_{n,k}\right) \to \mathcal{D}$ and $\psi\colon \mathcal{C}^{\mathsf{s-splt}}_p \cap \mathcal{C}^{\mathsf{s-me}}_{n,k} \to \mathcal{C}^{\mathsf{s-splt}}_p \cap \mathcal{C}^{\mathsf{s-me}}_{1,k}$, such that for every $(\mathsf{f},\mathsf{P}) \in \mathcal{C}^{\mathsf{s-splt}}_p \cap \mathcal{C}^{\mathsf{s-me}}_{n,k}$ we have*

$$\mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f},\mathsf{P},\sigma}(\mathsf{D}) \leq \binom{np}{2} 2^{-k} + n \cdot \mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f}',\mathsf{X}',\sigma}(\mathsf{D}')$$

*with $\mathsf{D}' \coloneqq \rho(\mathsf{D},\mathsf{f},\mathsf{P})$ and $(\mathsf{f}',\mathsf{X}') \coloneqq \psi(\mathsf{f},\mathsf{P})$.*

*Proof (Sketch).* The proof works very similarly to the one of Lemma 6.8 below; therefore, we only provide a brief sketch. As a first hybrid, we introduce a variant that uses a beacon instead of a random oracle, where a beacon is a resource with the same interface as the random oracle but always answers using fresh randomness even for repeated queries. Distinguishing this hybrid system from the ideal system (that uses the random oracle) can be bounded with the collision probability for the inputs. Since every of the input has $k$ bits of conditional min-entropy, given all previous inputs, the collision for any of them can be bounded with $2^{-k}$ (c.f. the proof below) and there are at most $np$ queries in total. Hence, the total distinction advantage can be bounded by $\binom{np}{2}2^{-k}$.

It remains to bound the distinction advantage between the real system (using the hash function) and our hybrid system (using the beacon) using the strong-split

**Converter $\mathsf{f}_{p,r}^{\mathsf{r-splt}}$**

**Initialization**

$b \leftarrow \bot^p$, $c \leftarrow 0$

**Outer Interface**

**Input:** `get`
  **output** $b$ at `out`
  $b \leftarrow \bot^p$

**Input:** $(\texttt{query}, f_1, \ldots, f_p) \in \mathcal{I}^p_{\mathcal{X},\mathcal{A} \to H.\mathcal{X}}$
  $c \leftarrow 1$
  **output** `retrieve` at `in.P`
  **if** the result can be parsed as $(x, a) \in \mathcal{X} \times \mathcal{A}$ **then**
    **for** $i = 1, \ldots, p$ **do**
      $y[i] \leftarrow f_i(x, a)$
    **if** $\forall i \neq j \colon y[i] \neq y[j]$ **then**
      **for** $i = 1, \ldots, n$ **do**
        **output** $y[i]$ at `in.H`
        let $b[i]$ denote the result
    **else**
      $b \leftarrow \bot^p$
  **else**
    $b \leftarrow \bot^p$

**Input:** $(\texttt{repeat}, f_1, \ldots, f_p) \in \mathcal{I}^p_{H.\mathcal{Y} \to H.\mathcal{X}}$
  $c \leftarrow c + 1$
  **if** $c \leq r \ \wedge \ b \neq \bot^p$ **then**
    **for** $i = 1, \ldots, p$ **do**
      **output** $f_i(b[i])$ at `in.H`
      let $b[i]$ denote the result
  **else**
    $b \leftarrow \bot^p$

Figure 11: The filter $\mathsf{f}_{p,r}^{\mathsf{r-splt}}$.

security for a single message. This can be shown by a simple hybrid-argument with $n$ additional hybrids where the $i$-th min-entropy seed $X_i$ outputs the $i$-th message $Y_i$ at interface `A` and the messages $Y_1, \ldots, Y_{i-1}$ as additional leakage at interface `E`. The hybrid then answers the first $i - 1$ queries by computing the hash function itself, the $i$-th message by actually querying the attached system (that uses either the hash function or the beacon), and the remaining queries by uniform random values, simulating the beacon. Defining the resource $\mathsf{X}'$ to be the one that chooses uniformly at random among $X_1, \ldots, X_n$ yields the desired bound: $n \cdot \mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f}',\mathsf{X}',\sigma_{\mathsf{H}}}(\mathsf{D}')$. □

## 6.5 The Repeated Split-Source Context Set

We now further generalize our strong-split source class, to allow for repeated queries, such as $H\big(hk, H(hk, x||1)||2\big)$. The key idea is to introduce a buffer which stores the results obtained from the hash function. The distinguisher can then choose whether it wants to see those values, or whether it wants to use them as a new query. The filter $\mathsf{f}_{p,r}^{\mathsf{r-splt}}$ is depicted in Figure 11. The parameter $r$ determines the maximal allowed nesting depth. Analogously to the strong-split source, we can then define the $\mathcal{C}_{p,r}^{\mathsf{r-splt}}$ context set based on this filter as $\mathcal{C}_{p,r}^{\mathsf{r-splt}} \coloneqq \{\mathsf{f} \circ \mathsf{f}_{p,r}^{\mathsf{r-splt}} \mid \mathsf{f} \in \Sigma\} \times \Phi^{\mathsf{ni}}$.

We now prove that strong-split CRI implies repeated-split CRI when furthermore restricted to strict min-entropy seeds. This allows to analyze hash functions only for strong-split security, but use them in contexts where repeated-split security is needed to implement a certain protocol.

**Lemma 6.8.** *Let $k' \coloneqq \min(k, \log|H.\mathcal{Y}|)$. If $H$ is a $\mathcal{C}_p^{\mathsf{s-splt}} \cap \mathcal{C}_{n,k'}^{\mathsf{s-me}}$ indifferentiable hash function, then $H$ is also $\mathcal{C}_{p,r}^{\mathsf{r-splt}} \cap \mathcal{C}_{n,k}^{\mathsf{s-me}}$ indifferentiable hash function.*

*More concretely, let $\mathcal{D}$ denote the set of distinguishers. Then there exists a translation of the distinguisher $\rho\colon \mathcal{D} \times \left(\mathcal{C}_{p,r}^{\mathsf{r-splt}} \cap \mathcal{C}_{n,k}^{\mathsf{s-me}}\right) \to \mathcal{D}$ and a translation of the context $\psi\colon \mathcal{C}_{p,r}^{\mathsf{r-splt}} \cap \mathcal{C}_{n,k}^{\mathsf{s-me}} \to \mathcal{C}_{p}^{\mathsf{s-splt}} \cap \mathcal{C}_{n,k'}^{\mathsf{s-me}}$, such that for every $(\mathsf{f},\mathsf{P}) \in \mathcal{C}_{p,r}^{\mathsf{r-splt}} \cap \mathcal{C}_{n,k}^{\mathsf{s-me}}$ we have*

$$\mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f},\mathsf{P},\sigma}(\mathsf{D}) \leq \binom{npr}{2} 2^{-(k'-1)} + r \cdot \mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f}',\mathsf{X}',\sigma}(\mathsf{D}')$$

*with $\mathsf{D}' \coloneqq \rho(\mathsf{D},\mathsf{f},\mathsf{P})$ and $(\mathsf{f}',\mathsf{X}') \coloneqq \psi(\mathsf{f},\mathsf{P})$.*

While this lemma can intuitively be proven using a simple hybrid argument, it turns out to be quite technical. The proof can be found in Appendix A.

### 6.6 The Relation Between ICE and Strong-Split CRI

In this section we discuss the relation between RO-CRI and the ICE framework introduced in [FM16]. More concretely, we show that statistical-unpredictable ICE security implies strong-split context-restricted indifferentiability, as phrased in Theorem 6.9. Using this relation between the two frameworks, we especially inherit the random oracle feasibility result from the ICE framework.

The reverse direction, whether strong-split RO-CRI implies some natural notion of ICE, remains an interesting open problem. In general, there seems to be no natural mapping from ICE to RO-CRI. This can be explained by the fundamentally different motivation behind introducing this two generalizations of UCE: ICE tried to allow interaction by making the two stages of UCE more symmetric, whereas RO-CRI exploits the asymmetry of UCE to separate them even further into the protocol of the honest party and the regular distinguisher from indifferentiability.

In terms of random-oracle feasibility, this places RO-CRI as an intermediate notion between the original UCE notion and the stronger ICE notion, while it is still open whether a true separation between those frameworks exists.

**Theorem 6.9.** *Let $\mathsf{H}$ denote a keyed hash function where the key-space is exponential in the security parameter. If $\mathsf{H} \in \text{ICE}[\mathcal{C}^{sup}]$, then $\mathsf{H}$ is $\mathcal{C}_{p}^{\mathsf{s-splt}} \cap \mathcal{C}_{n,k}^{\mathsf{s-me}}$ context-restricted indifferentiable from a random oracle for any polynomial $n$ and $p$, and $k$ such that the guessing probability is negligible.*

*Proof.* We sketch a proof that for the fixed simulator $\sigma_{\mathtt{H}}$, every context $(\mathsf{f},\mathsf{P}) \in \mathcal{C}_{p}^{\mathsf{s-splt}} \cap \mathcal{C}_{n,k}^{\mathsf{s-me}}$ and distinguisher $\mathsf{D}$ can be turned into a pair of equivalent ICE distinguishers $D_1$ and $D_2$. Let $D_1$ internally emulates the distinguisher $\mathsf{D}$ and works as follows:

- It initially chooses the hash key $hk$ uniformly at random (as $\sigma_{\mathtt{H}}$) and writes it into the buffer using a WRITE query. This is the only WRITE query $D_1$ does.
- In every round, it uses obtains the answer from $L_2$ and passes this to the distinguisher $\mathsf{D}$ to obtain the next query. According whether $\mathsf{D}$ queries the interface $\mathtt{A}$ with the function $f$ or obtains the leakage at interface $\mathtt{E}$, it produces an appropriate output $L_1$, either $(\mathtt{A}, f)$ or $(\mathtt{E})$.
- If the distinguisher $\mathsf{D}$ outputs the decision bit, $D_1$ outputs the same bit.

The second distinguisher $D_2$ internally emulates the context $(\mathsf{f}^{\mathsf{s-splt}},\mathsf{X})$. It works as follows:

- In every round it inspects the value $L_1$.

  - If $L_1$ is of the form $(\mathtt{A}, f)$, it passes $f$ to the internal emulation of the context, to obtain the value $x$ that would be queried to the hash function. It then writes $x$ to the buffer and queries the hash function. The resulting value $y$ is returned as $L_2$.
  - If $L_2$ is of the form $(\mathtt{E})$, then it queries the interface $\mathtt{E}$ of the internal resource $X$ and returns the result as $L_2$.

- It always sets $b_2 = 0$.

It is easy to see that the ICE game now behaves exactly the same as the RO-CRI system. Moreover, the queries of $D_2$ are exactly as unpredictable given the state and randomness of $D_1$ as are the queries in the RO-CRI system given access to the interface $\mathtt{E}$. Finally, if the hash key $hk$ is unpredictable, then none of the queries of $D_1$ can be predicted given the complete state and randomness of $D_2$. This concludes the proof. □

# 7 Split-Security of the Merkle-Damgård Construction

## 7.1 Motivation

Indifferentiability is widely used to prove the security of hash function constructions. Since CRI is essentially a refined version of indifferentiability, it is hence natural to consider the RO-CRI security as well.

It is easy to show that any indifferentiable hash function construction is reset-UCE secure if the underlying compression function is reset-UCE secure. On the other hand, for split security no corresponding result has been proven so far. In the following we investigate the split-security of the Merkle-Damgård construction using the RO-CRI framework. While ideally one could prove that the Merkle-Damgård construction is split secure if the compression function is so, or that the Merkle-Damgård construction is strong-split secure if the compression function is so, we will prove a slightly weaker result:

*Consider the Merkle-Damgård construction that splits the message into blocks of length $m$. We show that the Merkle-Damgård construction is split-secure for inputs having at least one block with $k$ bits of min-entropy, if the compression function is strong-split secure for inputs with* $\min(k, m)$ *bits of min-entropy.*

## 7.2 Formalizing the Theorem

In order for our proof to go through, we require that at least one of the blocks has high min-entropy and not just the overall message has, as in the definition of strict min-entropy seeds. Moreover, we require that this block has $k$ bits of min-entropy given all subsequent blocks. In Lemma 7.4 we then show that having a high min-entropy density, i.e., the fraction between the min-entropy and the message length, is a sufficient criteria for this. First, however, let us formally introduce this CRI context set.

**Definition 7.1.** For a block length $\ell \in \mathbb{N}_+$, let $\mathrm{Pad}_\ell$ denote the usual padding scheme of the Merkle-Damgård scheme, that is $\mathrm{Pad}_\ell \colon \{0,1\}^* \to (\{0,1\}^\ell)^+$ that pads a message $x$ by first appending zeros up to a multiple of the block length $\ell$, and then appending an encoding of the number of zeros appended as a last block. Moreover, for $X \in \{0,1\}^*$, we denote by $X^i$ the i-th block of $\mathrm{Pad}_\ell(X)$.

**Definition 7.2.** A non-interactive resource is said to be a $k$ *out of* $\ell$*-bit strict min-entropy block*, denoted $\mathsf{P} \in \Phi^{\mathsf{me-blk}}_{k,\ell,b,n}$, if $\mathsf{P} \in \Phi^{\mathsf{seed}}_{n}$ with $\bigcup_{i\leq(b-1)\ell}\{0,1\}^i \times \mathcal{A}$ as the output domain of interface $\mathtt{A}$, and there exist random variables $C_1, \ldots, C_n$ such that $C_i \in \{1, \ldots, \frac{|\mathrm{Pad}_\ell(X_i)|}{\ell}\}$ and

$$\forall i \leq n\colon\ \tilde{H}_\infty\big(X_i^{C_i} \,\big|\, \{X_i^j\}_{j>C_i}, \{X_j\}_{j<i}, \{C_j\}_{j\leq i}, \{A_j\}_{j\leq i}, Z\big) \ \geq\ k.$$

Moreover, let $\mathcal{C}^{\mathsf{me-blk}}_{k,\ell,b,n} \coloneqq \Sigma \times \Phi^{\mathsf{me-blk}}_{k,\ell,b,n}$.

*Remark.* Note, that contrary to the classical indifferentiability of the Merkle-Damgård construction, we do not require Pad to be prefix-free: when combined with the strict min-entropy condition $H(X)$ cannot be extended to $H(\mathrm{Pad}(X)||Y)$, as for $\mathrm{Pad}(X)||Y$ having high min-entropy given $X$, $Y$ must have so, and thereby the well-known length-extension attack is excluded. Whether a more advanced construction with a finalization function, e.g. HMAC, could be proven secure for a more relaxed context set remains an interesting open problem. We now phrase our main result of this section.

Using the definition of $k$ out of $\ell$-bit strict min-entropy block, we can now formally state our theorem about the split-security of the Merkle-Damgård construction.

**Theorem 7.3.** *Let* $h\colon \{0,1\}^{m+\ell} \to \{0,1\}^m$ *denote a fixed input-length compression function,* $H\colon \{0,1\}^* \to \{0,1\}^m$ *denote the hash function obtained by first padding the message using* $\mathrm{Pad}_\ell$ *and then applying the Merkle-Damgård scheme using* $h$*, and let* $k' \coloneqq \min(k, m)$*. Then, if* $h$ *is* $\mathcal{C}_1^{\mathsf{s-splt}} \cap \mathcal{C}_{1,k'}^{\mathsf{s-me}}$ *RO-CRI secure, then* $H$ *is* $\mathcal{C}^{\mathsf{splt}} \cap \mathcal{C}^{\mathsf{me-blk}}_{k,\ell,b,n}$ *RO-CRI secure for any polynomial* $b$ *and* $n$*.*

*More explicitly, there exists* $\rho_1, \rho_2\colon \mathcal{D} \times \big(\mathcal{C}^{\mathsf{splt}} \cap \mathcal{C}^{\mathsf{me-blk}}_{k,\ell,b,n}\big) \to \mathcal{D}$ *and* $\psi_1, \psi_2\colon \mathcal{C}^{\mathsf{splt}} \cap \mathcal{C}^{\mathsf{me-blk}}_{k,\ell,b,n} \to \mathcal{C}_1^{\mathsf{s-splt}} \cap \mathcal{C}_{1,k'}^{\mathsf{s-me}}$ *such that for all distinguishers* $\mathsf{D}$ *and all contexts* $(\mathsf{f}, \mathsf{P}) \in \mathcal{C}^{\mathsf{splt}} \cap \mathcal{C}^{\mathsf{me-blk}}_{k,\ell,b,n}$ *we have*

$$\mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f},\mathsf{P},\sigma}(\mathsf{D}) \leq \binom{n}{2} \cdot 2^{-k} + n \cdot \binom{b}{2} \cdot 2^{-(k'-1)} + nb \cdot \mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{h},\mathsf{f}',\mathsf{X}',\sigma'}(\mathsf{D}') + n \cdot \mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{h},\mathsf{f}'',\mathsf{X}'',\sigma''}(\mathsf{D}'')$$

*with* $\mathsf{D}' \coloneqq \rho_1(\mathsf{D}, \mathsf{f}, \mathsf{P})$*,* $\mathsf{D}'' \coloneqq \rho_2(\mathsf{D}, \mathsf{f}, \mathsf{P})$*,* $(\mathsf{f}', \mathsf{X}') \coloneqq \psi_1(\mathsf{f}, \mathsf{P})$*,* $(\mathsf{f}'', \mathsf{X}'') \coloneqq \psi_2(\mathsf{f}, \mathsf{P})$*, and* $\sigma'$ *and* $\sigma''$ *denoting slightly modified variants of* $\sigma$*.*

## 7.3 Proof of Theorem 7.3

Let us first provide an intuitive argument for the case of a single message. Assume that the message $y$ being hash by the Merkle-Damgård scheme is split into $b$ blocks, out of which at least one has $k$ bits of min-entropy. Let $c$ denote the index of this block, i.e., $y_c$ has at least $k$ bits of min-entropy. Hence, according to our assumption on the compression function, the output $q$ of this block cannot be distinguished from the output of a random oracle, as depicted in Figure 12. Given that this output is just a uniformly random value of length $m$, by induction, neither can be the output of any subsequent block be distinguished from the output of a random oracle. Therefore, the final output cannot be distinguished from the uniform random value $RO(X)$. We now proceed with the formal proof of Theorem 7.3.

*Proof of Theorem 7.3.* Using Lemma 6.6 it suffices to show

$$\mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f},\mathsf{P},\sigma}(\mathsf{D}) \leq \binom{b}{2} \cdot 2^{-(k'-1)} + b \cdot \mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{h},\mathsf{f}',\mathsf{X}',\sigma'}(\mathsf{D}') + \cdot \mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{h},\mathsf{f}'',\mathsf{X}'',\sigma''}(\mathsf{D}'')$$

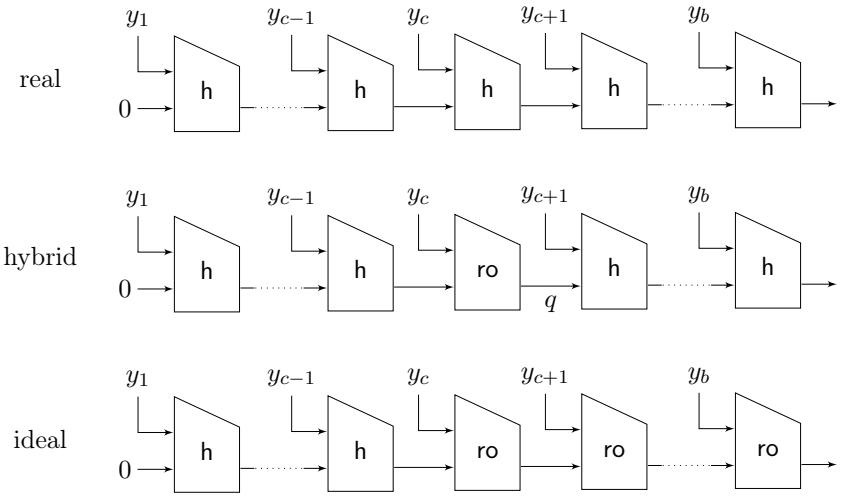



Figure 12: The real and the ideal setting for the Merkle-Damgård construction if block $c$ has high min-entropy.

for all distinguishers $\mathsf{D}$ and all contexts $(\mathsf{f}, \mathsf{P}) \in \mathcal{C}^{\mathsf{splt}} \cap \mathcal{C}^{\mathsf{me-blk}}_{k,\ell,1}$.

Next, observe that for any message $y \in \bigcup_{i \leq (b-1)\ell} \{0,1\}^i$, applying the padding $\mathrm{Pad}_\ell$ results in a message that has at most $b$ blocks. Without loss of generality, we assume in the following that there are always exactly $b$ blocks.

Given any $k$ out of $\ell$-bit min-entropy block seed $\mathsf{P}$ with a single output, we first introduce two $k'$-bit min-entropy seeds $\mathsf{X}'$ and $\mathsf{X}''$. Note that the function $\psi_1$ and $\psi_2$ are just mappings from one context to another one relating the two problems and, in contrast to the reduction translating the distinguisher, do not need to be efficiently computable. Therefore, it is sufficient to know that such a random variable $C$ from Definition 7.2 exists for the seed $\mathsf{X}$.

**Definition of $\mathsf{X}'$:**

Let $\mathsf{X}'$ denote the resource that samples $(y, z)$ using the same distribution as $\mathsf{P}$, applies the padding, and splits it into the blocks $y_1, \ldots, y_b$. Then, it sample the random variable $C$ to obtain the index $c$. Finally, it outputs the pair $(a', y')$ with $a' = (y_0, y_1, \ldots, y_{c-1})$ and $y' = y_c$ at interface $\mathtt{A}$ and $z' = (z, c, y_{c+1}, \ldots, y_b)$ at interface $\mathtt{E}$.

**Definition of $\mathsf{X}''$:**

Let $\mathsf{X}''$ denote the resource that samples $(y, z)$ using the same distribution as $\mathsf{P}$, applies the padding, and splits it into the blocks $y_1, \ldots, y_b$. Then, it sample the random variable $C$ to obtain the index $c$ and chooses $q \in \{0,1\}^m$ uniformly at random, outputs the pair $(a', y') := (\bot, q)$ at interface $\mathtt{A}$, and the value $z' := (z, c, y_{c+1}, \ldots, y_b)$ at interface $\mathtt{E}$.

Observe that $\mathsf{X}'$ is a $k \geq k'$ bit (strict) min-entropy seed, since $\mathsf{X}$ is $k$ out of $n$-bit min-entropy block seed. Similarly, since $q$ is chosen independently of all other random variables, the seed $\mathsf{X}''$ is a $m \geq k'$ bit strict min-entropy seed. Moreover, both of them output only a single value, i.e., $\mathsf{X}', \mathsf{X}'' \in \Phi^{\mathsf{s-me}}_{1,k'}$.

Next, we briefly sketch the two simulators $\sigma'$ and $\sigma''$: they both internally run $\sigma$. Whenever $\sigma$ request for the leakage $z$ of the seed, they query the leakage $z'$ at the corresponding inner interface and return the first component $z$ to $\sigma$.

Now, we introduce two converter systems $\mathsf{C}'$ and $\mathsf{C}''$ that at the inside interface

connect to both the interface A and the interface E of the connected system, and at the outside interface emulates both the interfaces as well.

**The system $\mathsf{C}'$ works as follows:**

First it obtains $hk$ and $z' = (z, c, y_{c+1}, \ldots, y_b)$ at the interfaces E.H and E.X of the connected system. When receiving the input retrieve at the outside interface A, it outputs (retrieve, $f$) at the inside interface A, where $f$ is the function that on input $(y_c, a')$ first splits $a' = (y_0, \ldots, y_{c-1})$, then computes the prefix $p = h_{hk}(\ldots h_{hk}(h_{hk}(0||y_0)||y_1)\ldots||y_{c-1})$, and finally returns $p||y_c$. Since both $p$ and $y_c$ are of fixed length, this function is injective in the first argument. When obtaining the returned value $y'$, it then computes the suffix $s = h_{hk}(\ldots h_{hk}(h_{hk}(y'||y_{c+1})||y_{c+2})\ldots||y_b)$ and returns $s$ at the outside interface A. When receiving the input retrieve at either the interface E.H or E.X it returns $hk$ or $z$, respectively.

**The system $\mathsf{C}''$ works as follows:**

First it obtains $hk$ and $z' = (z, c, x_{c+1}, \ldots, x_b)$ at the interfaces E.H and E.X of the connected system. When receiving the input retrieve at the outside interface A, it first outputs (query, $f$) at the inside interface A, where $f$ is the function that on input $(q, \perp)$ returns $q||y_{c+1}$. This function is injective in the first argument. Then, for $i = c+2, \ldots, b$ it outputs (repeat, $f$) at the inside interface A, where $f$ is the function that on input $(x)$ returns $x||y_i$. Finally, it outputs get at the inside interface A and returns the obtained value at the outside interface A. When receiving the input retrieve at either the interface E.H or E.R it returns $hk$ or $z$, respectively.

It is easy to verify, that the composed system $\mathsf{C}'\mathsf{f}^{\mathsf{s-splt}}[\mathsf{h}, \mathsf{X}']$ at the interface A outputs $H(y)$ and, thus, we have the equivalence $\mathsf{f}^{\mathsf{splt}}[\mathsf{H}, \mathsf{P}] \equiv \mathsf{C}'\mathsf{f}^{\mathsf{s-splt}}[\mathsf{h}, \mathsf{X}']$. In the following $\mathsf{f}_{1,p}^{\mathsf{r-splt}}$ denote the filter introduced in Section 6.5. It is then easy to verify that the final output of the composed system $\mathsf{C}''\mathsf{f}_{1,p}^{\mathsf{r-splt}}[\mathsf{ro}, \mathsf{X}'']\sigma''$ at the interface A is just a uniform random value independent of $hk$ and $z$. Hence, this system behaves equivalently to $\mathsf{f}^{\mathsf{splt}}[\mathsf{RO}, \mathsf{X}]\sigma$ that outputs a single uniform random value as well. In short, we have $\mathsf{f}^{\mathsf{splt}}[\mathsf{RO}, \mathsf{X}]\sigma \equiv \mathsf{C}''\mathsf{f}_{1,p}^{\mathsf{r-splt}}[\mathsf{ro}, \mathsf{X}'']\sigma''$.

Using those two equivalences, and by introducing two hybrids $\mathsf{C}'\mathsf{f}_1^{\mathsf{s-splt}}[\mathsf{ro}, \mathsf{X}']\sigma'$ and $\mathsf{C}''\mathsf{f}_{1,b}^{\mathsf{r-splt}}[\mathsf{h}, \mathsf{X}'']\sigma''$, we can rewrite the distinction advantage as:

$$\begin{aligned}\Delta^{\mathsf{D}}(\mathsf{f}^{\mathsf{splt}}[\mathsf{H}, \mathsf{P}], \mathsf{f}^{\mathsf{splt}}[\mathsf{RO}, \mathsf{P}]\sigma) = {} & \Delta^{\mathsf{D}}(\mathsf{C}'\mathsf{f}_1^{\mathsf{s-splt}}[\mathsf{h}, \mathsf{X}'], \mathsf{C}'\mathsf{f}_1^{\mathsf{s-splt}}[\mathsf{ro}, \mathsf{X}']\sigma') \\ & + \Delta^{\mathsf{D}}(\mathsf{C}'\mathsf{f}_1^{\mathsf{s-splt}}[\mathsf{ro}, \mathsf{X}']\sigma', \mathsf{C}''\mathsf{f}_{1,\mathsf{b}}^{\mathsf{r-splt}}[\mathsf{h}, \mathsf{X}'']) \\ & + \Delta^{\mathsf{D}}(\mathsf{C}''\mathsf{f}_{1,\mathsf{b}}^{\mathsf{r-splt}}[\mathsf{h}, \mathsf{X}''], \mathsf{C}''\mathsf{f}_{1,\mathsf{b}}^{\mathsf{r-splt}}[\mathsf{ro}, \mathsf{X}'']\sigma'').\end{aligned}$$

Finally, observe that the systems $\mathsf{C}'\mathsf{f}_1^{\mathsf{s-splt}}[\mathsf{ro}, \mathsf{X}']\sigma'$ and $\mathsf{C}''\mathsf{f}_{1,b}^{\mathsf{r-splt}}[\mathsf{h}, \mathsf{X}'']\sigma''$ both implement exactly the same hybrid system depicted in Figure 12: The system $\mathsf{C}'\mathsf{f}_1^{\mathsf{s-splt}}[\mathsf{ro}, \mathsf{X}']\sigma'$ actually computes this value by first using the compression function $h$ on the blocks 1 to $c-1$, then uses the fixed input size random oracle on the block $c$, and finishes by using $h$ on the remaining blocks. However, note that the value output by $\mathsf{ro}$ is just a uniform random value, as $\mathsf{ro}$ is private and not used beside this one query. The system $\mathsf{C}''\mathsf{f}_{1,b}^{\mathsf{r-splt}}[\mathsf{h}, \mathsf{X}'']$ skips the initial computes and chooses $q$ uniformly at random (in $\mathsf{X}''$).

As a result, we can simplify the distinction advantage to

$$\Delta^{\mathsf{D}}(\mathsf{f}^{\mathsf{splt}}[\mathsf{H},\mathsf{P}],\mathsf{f}^{\mathsf{splt}}[\mathsf{RO},\mathsf{P}]\sigma) = \Delta^{\mathsf{DC}'}(\mathsf{f}_1^{\mathsf{s-splt}}[\mathsf{h},\mathsf{X}'],\mathsf{f}_1^{\mathsf{s-splt}}[\mathsf{ro},\mathsf{X}']\sigma') + \Delta^{\mathsf{DC}''}(\mathsf{f}_{1,\mathsf{b}}^{\mathsf{r-splt}}[\mathsf{h},\mathsf{X}''],\mathsf{f}_{1,\mathsf{b}}^{\mathsf{r-splt}}[\mathsf{ro},\mathsf{X}'']\sigma'').$$

Applying the definition of $\mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f},\mathsf{P},\sigma}(\mathsf{D})$, Lemma 6.3, and Lemma 6.8 (with $r = b$, $n = 1$, and $p = 1$) concludes the proof. □

## 7.4 A Sufficient Condition Based on Min-Entropy Splitting

To conclude this section, we now present a sufficient condition for a seed to satisfy Definition 7.2 based on the length of the message and its overall min-entropy. More concretely, we prove that if a message is split into $b$ blocks of size $n$, and has overall min-entropy of $k$ bits, then there exists a block with $\frac{k}{b} - \log_2(b)$ bits of min-entropy, given all succeeding blocks. In order to more closely resembles the chain rule of Shannon entropy, the proposition is stated with conditioning on all preceding message $X_1 \dots X_{C-1}$ instead of all succeeding ones. The converse result can easily be obtained by simply relabeling the blocks.

**Lemma 7.4.** *Let $X_1, \dots, X_b$ and $Z$ be random variables (over possibly different alphabets) with $\tilde{H}_\infty(X_1 \dots X_b \,|\, Z) \geq k$. Then, there exists a random variable $C$ over the set $\{1, \dots, b\}$ such that $\tilde{H}_\infty(X_C \,|\, X_1 \dots X_{C-1} C Z) \geq k/b - \log_2(b)$.*

*Proof.* Let $Y_C \coloneqq (X_1, \dots, X_{C-1})$, with $Y_0$ denoting the empty string $\lambda$. Second, let for every $z$ in the support of $Z$,

$$p_z \coloneqq \max_{x_1,\dots,x_b} \mathsf{P}_{X_1 \dots X_b | Z}(x_1, \dots, x_b, z),$$

that is, $\tilde{H}_\infty(X_1 \dots X_b \,|\, Z) = -\log \mathbb{E}_z[p_z]$. Moreover, once $C$ is defined (see below), let

$$q_z \coloneqq \mathbb{E}_{c,y}[\max_x \mathsf{P}_{X_C | C Y_C Z}(x, c, y, z) \,|\, Z = z]$$

and note that $\tilde{H}_\infty(X_C \,|\, C Y_C Z) = -\log \mathbb{E}_z[q_z]$. We now proceed by showing that for all $z$, $q_z \leq b \cdot p_z^{1/b}$. To this end, we extend the probability distribution $\mathsf{P}_{X_1 \dots X_b Z}$ by defining the random variable $C$ as follows:

$$C = \begin{cases} 1 & \text{if } \mathsf{P}_{X_1|Z}(x_1, z) < p_z^{1/b} \\ 2 & \text{else if } \mathsf{P}_{X_1 X_2|Z}(x_1, x_2, z) < p_z^{2/b} \\ \vdots & \\ b-1 & \text{else if } \mathsf{P}_{X_1 \dots X_{k-1}|Z}(x_1, \dots, x_{b-1}, z) < p_z^{(b-1)/k} \\ b & \text{else.} \end{cases}$$

Observe that with

$$\mathcal{Y}_{c,z} \coloneqq \{y \mid \mathsf{P}_{C Y_C | Z}(c, y, z) > 0\}$$
$$\mathcal{X}_{c,z,y} \coloneqq \{x \mid \mathsf{P}_{X_C C Y_C | Z}(x, c, y, z) > 0\}$$

we can bound $q_z$ as follows:

$$\begin{aligned}
q_z &= \mathbb{E}_{c,y}[\max_x \mathsf{P}_{X_C|CY_CZ}(x,c,y,z) \mid Z=z] \\
&= \sum_{c=1}^{b} \sum_{y\in\mathcal{Y}_{c,z}} \mathsf{P}_{CY_C|Z}(c,y,z) \cdot \max_{x\in\mathcal{X}_{c,z,y}} \mathsf{P}_{X_C|CY_CZ}(x,c,y,z) \\
&= \sum_{c=1}^{b} \sum_{y\in\mathcal{Y}_{c,z}} \mathsf{P}_{CY_C|Z}(c,y,z) \cdot \max_{x\in\mathcal{X}_{c,z,y}} \frac{\mathsf{P}_{X_CCY_C|Z}(x,c,y,z)}{\mathsf{P}_{CY_C|Z}(c,y,z)} \\
&= \sum_{c=1}^{b} \sum_{y\in\mathcal{Y}_{c,z}} \max_{x\in\mathcal{X}_{c,z,y}} \mathsf{P}_{X_CCY_C|Z}(x,c,y,z) \\
&\leq \sum_{c=1}^{b} \sum_{y\in\mathcal{Y}_{c,z}} \max_{x\in\mathcal{X}_{c,z,y}} \mathsf{P}_{X_CY_C|Z}(x,y,z).
\end{aligned}$$

We now further bound this term using a case distinction on $c$. First, consider the case $c=1$. Since $Y_1=\lambda$ is constant, we have $\mathcal{Y}_{1,z}\subseteq\{\lambda\}$ and $\mathsf{P}_{X_1Y_1|Z}(x,\lambda,z)=\mathsf{P}_{X_1|Z}(x,z)$. Moreover, $x\in\mathcal{X}_{1,z,\lambda}$ implies $\mathsf{P}_{X_1C|Z}(x,1,z)>0$, which by the definition of $C$ in turn implies $\mathsf{P}_{X_1|Z}(x,z)<p_z^{1/b}$. Hence

$$\sum_{y\in\mathcal{Y}_{1,z}} \max_{x\in\mathcal{X}_{1,z,y}} \mathsf{P}_{X_1Y_1|Z}(x,y,z) \leq \max_{x\in\mathcal{X}_{1,z,\lambda}} \mathsf{P}_{X_1|Z}(x,z) \leq p_z^{1/b}.$$

For all $i\in\{2,\ldots,b-1\}$ observe that by the definition of $C$ we have that $\mathcal{X}_{i,z,y}\subseteq\left\{x \mid \mathsf{P}_{X_iY_i|Z}(x,y,z)<p_z^{i/b}\right\}$ and $\mathcal{Y}_{i,z}\subseteq\left\{y \mid \mathsf{P}_{Y_i|Z}(y,z)\geq p_z^{(i-1)/b}\right\}$. From the latter we can conclude that $|\mathcal{Y}_{i,z}|\leq\frac{1}{p_z^{(i-1)/b}}$ and, hence, we obtain

$$\sum_{y\in\mathcal{Y}_{i,z}} \max_{x\in\mathcal{X}_{i,z,y}} \mathsf{P}_{X_iY_i|Z}(x,y,z) \leq \sum_{y\in\mathcal{Y}_{i,z}} p_z^{i/b} \leq \frac{p_z^{i/b}}{p_z^{(i-1)/b}} = p_z^{1/b}.$$

Finally, for $c=b$, we have that $\mathcal{Y}_{b,z}\subseteq\{y \mid \mathsf{P}_{Y_b|Z}(y,z)\geq p_z^{(b-1)/b}\}$ and, therefore, we obtain $|\mathcal{Y}_{b,z}|\leq\frac{1}{p_z^{(b-1)/b}}$. Using the definition of $Y_b=(X_1,\ldots,X_{b-1})$ and $p_z$, we get $\max_{x\in\mathcal{X}_{b,z,y}}\mathsf{P}_{X_bY_b|Z}(x,y,z)\leq p_z$ for every $y=(x_1,\ldots,x_{b-1})$. Hence,

$$\sum_{y\in\mathcal{Y}_{b,z}} \max_{x\in\mathcal{X}_{b,z,y}} \mathsf{P}_{X_bY_b|Z}(x,y,z) \leq \sum_{y\in\mathcal{Y}_{b,z}} p_z \leq \frac{p_z}{p_z^{(b-1)/b}} = p_z^{1/b}$$

as well. In summary,

$$\begin{aligned}
q_z &= \mathbb{E}_{c,y}[\max_x \mathsf{P}_{X_C|CY_CZ}(x,c,y,z) \mid Z=z] \\
&\leq \sum_{c=1}^{b} \sum_{y\in\mathcal{Y}_{c,z}} \max_{x\in\mathcal{X}_{c,z,y}} \mathsf{P}_{X_CY_C|Z}(x,y,z) \\
&\leq \sum_{c=1}^{b} p_z^{1/b} \\
&\leq b\cdot p_z^{1/b}
\end{aligned}$$

Using the monotonicity of the expected value, Jensen's inequality, and the assumed inequality $\tilde{H}_\infty(X_1 \dots X_b \mid Z) \geq k$ yields

$$\begin{aligned} 2^{-\tilde{H}_\infty(X_C|CY_CZ)} &= \mathbb{E}_z[q_z] \leq \mathbb{E}_z[b \cdot p_z^{1/b}] \leq b \cdot \mathbb{E}_z[p_z]^{1/b} \\ &= b \cdot \left(2^{-\tilde{H}_\infty(X_1 \dots X_b|Z)}\right)^{1/b} \leq 2^{\log b} \cdot 2^{-k/b} = 2^{-(k/b - \log b)} \end{aligned}$$

concluding the proof. □

This lemma is a generalization of the randomized chain rule proven by the authors of [DFR+07] (similar variants exists also in [BK12; Wul07]) stating that there exists a binary random variable $C$ such that $H_\infty(X_{1-C}C) \geq H_\infty(X_0X_1)/2$. Note that the main difference of our result is, that it conditions on all previous blocks, i.e., it essentially represents the min-entropy equivalence of the strong chain rule $H(X_0) + H(X_1 \mid X_0) = H(X_0X_1)$ instead of $H(X_0) + H(X_1) \geq H(X_0X_1)$.

## 8 Conclusion

In this work, we have introduced the *context-restricted indifferentiability* framework that introduces the concept of "semi-composability", i.e., it allows to phrase explicitely in which contexts a resource can be instantiated with an construction. This stands in stark contrast to both the usual composable frameworks that ensure a resource can be instantiated in all contexts, and most game-based definitions where the composition guarantees are rather concealed.

While the CRI framework is defined as a generalization of indifferentiability, as a first result we have shown that it generalizes the UCE framework as well, thereby proposing an alternative view on the multi-stage definition of UCE. Moreover, we have shown how our alternative view can lead to meaningful generalizations of UCE that do allow some restricted interaction between the source and the distinguisher, introducing the notion of strong-split security as an example.

Finally, we proposed to use CRI as a fine grained version of indifferentiability to analyze the soundness of hash-function constructions and investigated the split-security of the Merkle-Damgård construction as an example. In general, we believe that using CRI can shed some more light on the security of various well-known and proposed constructions in a similar way considering indifferentiability instead of just collision resistance did.

## A Proof of Lemma 6.8

**Lemma 6.8.** *Let $k' \coloneqq \min(k, \log|H.\mathcal{Y}|)$. If $H$ is a $\mathcal{C}_p^{\mathsf{s-splt}} \cap \mathcal{C}_{n,k'}^{\mathsf{s-me}}$ indifferentiable hash function, then $H$ is also $\mathcal{C}_{p,r}^{\mathsf{r-splt}} \cap \mathcal{C}_{n,k}^{\mathsf{s-me}}$ indifferentiable hash function.*

*More concretely, let $\mathcal{D}$ denote the set of distinguishers. Then there exists a translation of the distinguisher $\rho\colon \mathcal{D} \times \left(\mathcal{C}_{p,r}^{\mathsf{r-splt}} \cap \mathcal{C}_{n,k}^{\mathsf{s-me}}\right) \to \mathcal{D}$ and a translation of the context $\psi\colon \mathcal{C}_{p,r}^{\mathsf{r-splt}} \cap \mathcal{C}_{n,k}^{\mathsf{s-me}} \to \mathcal{C}_p^{\mathsf{s-splt}} \cap \mathcal{C}_{n,k'}^{\mathsf{s-me}}$, such that for every $(\mathsf{f}, \mathsf{P}) \in \mathcal{C}_{p,r}^{\mathsf{r-splt}} \cap \mathcal{C}_{n,k}^{\mathsf{s-me}}$ we have*

$$\mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f},\mathsf{P},\sigma}(\mathsf{D}) \leq \binom{npr}{2} 2^{-(k'-1)} + r \cdot \mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f}',\mathsf{X}',\sigma}(\mathsf{D}')$$

*with $\mathsf{D}' \coloneqq \rho(\mathsf{D}, \mathsf{f}, \mathsf{P})$ and $(\mathsf{f}', \mathsf{X}') \coloneqq \psi(\mathsf{f}, \mathsf{P})$.*

*Proof.* Let $(\mathsf{f},\mathsf{P}) \in \mathcal{C}_{p,r}^{\mathsf{r-splt}} \cap \mathcal{C}_{n,k}^{\mathsf{s-me}}$. By definition, we then have $\mathsf{f} \coloneqq \mathsf{g} \circ \mathsf{f}_{p,r}^{\mathsf{r-splt}}$ for some filter $\mathsf{g}$. This filter can also be thought of as an reduction of the distinguisher (which follows from the composition-order independence [MR11]), and thus we can rewrite

$$\begin{aligned}\mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f},\mathsf{P},\sigma}(\mathsf{D}) \coloneqq& \Delta^{\mathsf{D}}(\mathsf{f}[\mathsf{H},\mathsf{P}], \mathsf{f}[\mathsf{RO},\mathsf{P}]\sigma) \\ =& \Delta^{\mathsf{D}''}(\mathsf{f}_{\mathsf{p,r}}^{\mathsf{r-splt}}[\mathsf{H},\mathsf{P}], \mathsf{f}_{\mathsf{p,r}}^{\mathsf{r-splt}}[\mathsf{RO},\mathsf{P}]\sigma)\end{aligned}$$

with $\mathsf{D}'' = \rho_1(\mathsf{D}) \coloneqq \mathsf{Dg}$.

Consider the beacon resource $\mathsf{B}$ that has the same interface as the random oracle interface, but response with a fresh random value for each query (i.e., it ignores the consistency condition for repeated queries). Moreover, we introduce the following shorthand notation: $\mathsf{S}^{\mathsf{H}} \coloneqq \mathsf{f}_{p,r}^{\mathsf{r-splt}}[\mathsf{H},\mathsf{P}]$, $\mathsf{S}^{\mathsf{RO}} \coloneqq \mathsf{f}_{p,r}^{\mathsf{r-splt}}[\mathsf{RO},\mathsf{P}]\sigma$, and $\mathsf{S}^{\mathsf{B}} \coloneqq \mathsf{f}_{p,r}^{\mathsf{r-splt}}[\mathsf{B},\mathsf{P}]\sigma$, which allows the advantage of the distinguisher $\mathsf{D}''$ to be expressed as

$$\Delta^{\mathsf{D}''}(\mathsf{f}[\mathsf{H},\mathsf{P}], \mathsf{f}[\mathsf{RO},\mathsf{P}]\sigma) = \Delta^{\mathsf{D}''}(\mathsf{S}^{\mathsf{H}}, \mathsf{S}^{\mathsf{B}}) + \Delta^{\mathsf{D}''}(\mathsf{S}^{\mathsf{B}}, \mathsf{S}^{\mathsf{RO}}).$$

We now describe the reduction $\rho_2$ that bounds the first term of the sum with $\binom{npr}{2}2^{-k'} + r \cdot \mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f}',\mathsf{X}',\sigma}(\mathsf{D}')$ using a simple hybrid argument.

Let $\{\mathsf{X}_\mathsf{i}\}_{i\in[q]}$ denote the sequence of hybrid resources that behave as follows: at the interface $\mathtt{E}$, the resource first outputs the index $i$ and subsequently behaves exactly as $\mathsf{P}$. At the interface $\mathtt{A}$, if $i = 1$ then it behaves exactly as $\mathsf{P}$, and if $i > 1$ then it outputs $n$ independent uniformly at random chosen values from the set $H.\mathcal{Y}$. It is easy to see, that if $\mathsf{P} \in \Phi_{n,k'}^{\mathsf{s-me}}$, then $\mathsf{X}_\mathsf{i} \in \Phi_{n,k'}^{\mathsf{s-me}}$ for all $i$. In addition, let $\mathsf{X}'$ denote the resource which chooses $i \in [q]$ uniformly at random and then behaves like $\mathsf{X}_\mathsf{i}$. Furthermore, let $\mathsf{f}' \coloneqq \mathsf{f}_p^{\mathsf{s-splt}}$ and, hence $(\mathsf{f}',\mathsf{X}') \in \mathcal{C}_p^{\mathsf{s-splt}} \cap \mathcal{C}_{n,k'}^{\mathsf{s-me}}$. Analogously to above, let us define the following shorthand notation: $\mathsf{T}^{\mathsf{H}} \coloneqq \mathsf{f}_p^{\mathsf{s-splt}}[\mathsf{R},\mathsf{X}']$, $\mathsf{T}_\mathsf{i}^{\mathsf{H}} \coloneqq \mathsf{f}_p^{\mathsf{s-splt}}[\mathsf{R},\mathsf{X}_\mathsf{i}]$, and $\mathsf{T}^{\mathsf{R}} \coloneqq \mathsf{f}_p^{\mathsf{s-splt}}[\mathsf{R},\mathsf{X}']\sigma$ and $\mathsf{T}_\mathsf{i}^{\mathsf{R}} \coloneqq \mathsf{f}_p^{\mathsf{s-splt}}[\mathsf{R},\mathsf{X}_\mathsf{i}]\sigma$ for $\mathsf{R} \in \{\mathsf{RO},\mathsf{B}\}$.

Now, consider the reduction $\mathsf{D}' \coloneqq \rho_2(\mathsf{D}'') = \rho_2(\rho_1(\mathsf{D}))$ where $\rho_2$ is implemented using a special type of system $\mathsf{C}$ that translates one setting into the other. Formally $\mathsf{C}$ is a converter that has an inside and an outside interface, where the inside interface connects to all the (merged) interfaces of the attached resource (here interface $\mathtt{A}$ and $\mathtt{E}$) and the outside interface becomes the interfaces of the composed resource. Now consider the following reduction system $\mathsf{C}$, which on the inside expects to be connected either to the resource $\mathsf{T}_\mathsf{i}^{\mathsf{H}}$ or $\mathsf{T}_\mathsf{i}^{\mathsf{B}}$. At the outside interfaces, it simulates the according interfaces of $\mathsf{f}_{p,r}^{\mathsf{r-splt}}[\mathsf{H},\mathsf{P}]$ and $\mathsf{f}_{p,r}^{\mathsf{r-splt}}[\mathsf{B},\mathsf{P}]\sigma$. The system $\mathsf{C}$ first gets the index $i$ and the hash key $hk$ at the inside interface. In every sequence of queries of the form $(\mathtt{query}, f_1), (\mathtt{repeat}, f_2), (\mathtt{repeat}, f_3), \ldots$, the queries 1 to $i-1$ are simulated internally as queries to the beacon by sampling a value uniformly at random and storing it in a buffer $b$. The $i$-th query in each such sequence is then answered using the actual resource connected at the inside interface. For the remaining queries, the system $\mathsf{C}$ computes the hash function $H$ itself. A formal description of the reduction system is provided in Figure 13.

The following system equivalences are easy to verify:

$$\mathsf{CT}_1^{\mathsf{H}} \equiv \mathsf{S}^{\mathsf{H}} \tag{1}$$

$$\mathsf{CW}_\mathsf{r}^{\mathsf{B}} \equiv \mathsf{S}^{\mathsf{B}} \tag{2}$$

$$\mathsf{CW}_{\mathsf{i}-1}^{\mathsf{B}} \equiv \mathsf{CW}_\mathsf{i}^{\mathsf{H}} \quad \forall i \in \{2,\ldots,q\}. \tag{3}$$

**Resource C**

**Initialization**

$b \leftarrow \perp^p$
$j \leftarrow 0$
**output** `retrieve` at `in.E.H`
let $hk$ denote the result
**output** `retrieve` at `in.E.X`
let $i$ denote the result

**Outer Interface `A`**

**Input:** `get`
**output** $b$ at `out.A`
$b \leftarrow \perp^p$

**Input:** $(\texttt{query}, f_1, \ldots, f_p)$
$j \leftarrow 1$
**if** $i = 1$ **then**
**output** $(\texttt{retrieve}, f_1, \ldots, f_p)$ at `in.A`
let $b$ denote the result
**else**
$b \xleftarrow{\$} H.\mathcal{Y}^p$

**Input:** $(\texttt{repeat}, f_1, \ldots, f_p)$
$j \leftarrow j + 1$
**if** $b \neq \perp^p$ **then**
**for** $\ell = 1, \ldots, p$ **do**
**if** $j < i$ **then**
$b[\ell] \xleftarrow{\$} H.\mathcal{Y}$
**else if** $j = i$ **then**
**output** $(\texttt{retrieve}, (x, a) \mapsto f_\ell(x))$ at `in.A`
let $b[\ell]$ denote the result
**else**
$b[\ell] \leftarrow H(hk, f_l(b[\ell]))$

**Outer Interface `E.i`** $i \in \{H, X\}$

**Input:** `retrieve`
**output** `retrieve` at `in.E.i`
let $y$ denote the result
**output** $y$ at `out.E.i`

Figure 13: The reduction system C.

As a consequence, we can rewrite the second term as

$$\begin{aligned}
\Delta^{\mathsf{D}''}(\mathsf{S}^{\mathsf{H}}, \mathsf{S}^{\mathsf{B}}) &= \Delta^{\mathsf{D}''}(\mathsf{CT}_1^{\mathsf{H}}, \mathsf{CT}_{\mathsf{r}}^{\mathsf{B}}) \\
&= \Delta^{\mathsf{D}''}(\mathsf{CT}_1^{\mathsf{H}}, \mathsf{CT}_1^{\mathsf{B}}) + \Delta^{\mathsf{D}''}(\mathsf{CT}_1^{\mathsf{B}}, \mathsf{CT}_2^{\mathsf{H}}) \\
&\quad + \Delta^{\mathsf{D}''}(\mathsf{CT}_2^{\mathsf{H}}, \mathsf{CT}_2^{\mathsf{B}}) + \Delta^{\mathsf{D}}(\mathsf{CT}_2^{\mathsf{B}}, \mathsf{CT}_3^{\mathsf{H}}) \\
&\quad + \dots \\
&\quad + \Delta^{\mathsf{D}}(\mathsf{CT}_{\mathsf{r}}^{\mathsf{H}}, \mathsf{CT}_{\mathsf{r}}^{\mathsf{B}}) \\
&= \sum_{i=1}^{r} \Delta^{\mathsf{D}''}(\mathsf{CT}_{\mathsf{i}}^{\mathsf{H}}, \mathsf{CT}_{\mathsf{i}}^{\mathsf{B}}) \\
&= r \cdot \Delta^{\mathsf{D}''}(\mathsf{CT}^{\mathsf{H}}, \mathsf{CT}^{\mathsf{B}}) \\
&= r \cdot \Delta^{\mathsf{D}'}(\mathsf{T}^{\mathsf{H}}, \mathsf{T}^{\mathsf{B}}) \\
&= r \cdot \mathbf{Adv}^{\text{RO-CRI}}_{\mathsf{H},\mathsf{f}',\mathsf{R}',\sigma}(\mathsf{D}') + r \cdot \Delta^{\mathsf{D}'}(\mathsf{T}^{\mathsf{RO}}, \mathsf{T}^{\mathsf{B}})
\end{aligned}$$

where in the third step we used Equation (3). In the forth step we used that the distinguishing advantage of $\mathsf{D}''$ on the problem with $\mathsf{R}'$ is the average of the distinguising advantage of $\mathsf{D}$ on resources with the the fixed $i$. Hence, the sum of these $r$ terms is equal to $r$ times the average.

The overall claim is then directly implied by the following two bounds, which remain to be shown:

$$\Delta^{\mathsf{D}'}(\mathsf{T}^{\mathsf{RO}}, \mathsf{T}^{\mathsf{B}}) \leq \binom{np}{2} 2^{-k'} \tag{4}$$

$$\Delta^{\mathsf{D}''}(\mathsf{S}^{\mathsf{B}}, \mathsf{S}^{\mathsf{RO}}) \leq \binom{npr}{2} 2^{-k'} \tag{5}$$

In both cases the two resources behave exactly identically until a repeated query to the oracle occurs. Hence, we can bound the distinction advantage by the probability of managing non-adaptively to query twice the same input [Mau13]. In the following, we only prove 5, as 4 follows by an analogous argument.

Let $Z_1, Z_2, \dots, Z_{npr}$ denote the queries, which are submitted to the beacon. The collision probability can then be bounded using the union bound

$$\Pr(\exists i \neq j \;\; Z_i = Z_j) \leq \sum_{i \neq j} \Pr(Z_i = Z_j).$$

Observe that all queries are either of the form $f(Y_s, A_s)$, where $(Y_s, A_s)$ is the $s$-th pair output by the entropy source, or $f(Y)$, where $Y$ is an output of the beacon. If either $Z_i$ or $Z_j$ is of the latter type, then the collision probability is trivially upper bounded by $\frac{1}{|H.\mathcal{Y}|} \leq 2^{-k'}$, using that $f$ is injective. If both of them are of the former type, then that by definition of the filter $\mathsf{f}^{\mathsf{r-splt}}_{p,r}$ the two inputs $Z_i$, $Z_j$ cannot collide if they depend on the same underlying value $X_s$ from the entropy source. Hence, assume w.l.o.g. that $Y_i = f(Y_s, A_s)$ and $Y_j = f(Y_t, A_t)$ with $s > t$. For every pair of

fixed auxiliary information $(a_s, a_t)$, we obtain the following bound:

$$\begin{aligned}
&\Pr(f_i(Y_s, a_s) = f_j(Y_t, a_t)) \\
&= \sum_z \Pr(f_i(Y_s, a_s) = z \wedge f_j(Y_t, a_t) = z) \\
&= \sum_z \Pr(Y_t = f_j^{-1}(z, a_t)) \cdot \Pr(Y_s = f_i^{-1}(z, a_s) \mid Y_t = f_j^{-1}(z, a_t)) \\
&\leq \sum_z \Pr(Y_t = f_j^{-1}(z, a_t)) \cdot \max_{t_s} \Pr(Y_s = t_s \mid Y_t = f_j^{-1}(z, a_t)) \\
&= \sum_{y_t} \Pr(Y_t = y_t) \cdot \max_{y_s} \Pr(Y_s = y_s \mid Y_t = y_t) \\
&= 2^{-\tilde{H}_\infty(Y_s|Y_t)} = 2^{-k} \leq 2^{-k'}.
\end{aligned}$$

Averaging over the choice of $(a_s, a_t)$ yields the desired result

$$\Pr(f_i(Y_s, A_s) = f_j(Y_t, A_t)) \leq 2^{-k'},$$

and in summary, the distinction advantage $\Delta^{\mathsf{D}}(\mathsf{S}^{\mathsf{B}}, \mathsf{S}^{\mathsf{RO}})$ can be bounded as

$$\Pr(\exists i \neq j \;\; Z_i = Z_j) \leq \sum_{i \neq j} \Pr(Z_i = Z_j) \leq \binom{npr}{2} 2^{-k'}. \qquad \square$$

## References


[BHK13] M. Bellare, V. T. Hoang, and S. Keelveedhi, "Instantiating Random Oracles via UCEs", in *Advances in Cryptology – CRYPTO 2013*, Springer Berlin Heidelberg, 2013, pp. 398–415.

[BHK14] ——, "Cryptography from compression functions: The UCE bridge to the ROM", in *Advances in Cryptology – CRYPTO 2014*. Springer Berlin Heidelberg, 2014, pp. 169–187.

[BR93] M. Bellare and P. Rogaway, "Random oracles are practical: A Paradigm for Designing Efficient Protocols", in *1st ACM Conference on Computer and Communications Security – CCS 93*, ACM Press, 1993, pp. 62–73.

[BST16] M. Bellare, I. Stepanovs, and S. Tessaro, "Contention in Cryptoland: Obfuscation, Leakage and UCE", in *Theory of Cryptography – TCC 2016-A*, Springer Berlin Heidelberg, 2016, pp. 542–564.

[BK12] Z. Brakerski and Y. Kalai, "A parallel repetition theorem for leakage resilience", in *Theory of Cryptography – TCC 2012*, Springer Berlin Heidelberg, 2012, pp. 248–265.

[BFM14] C. Brzuska, P. Farshim, and A. Mittelbach, "Indistinguishability Obfuscation and UCEs: The Case of Computationally Unpredictable Sources", in *Advances in Cryptology – CRYPTO 2014*, Springer Berlin Heidelberg, 2014, pp. 188–205.

[BM14] C. Brzuska and A. Mittelbach, "Using Indistinguishability Obfuscation via UCEs", in *Advances in Cryptology – ASIACRYPT 2014*, Springer Berlin Heidelberg, 2014, pp. 122–141.

[BM15] ——, *Universal Computational Extractors and the Superfluous Padding Assumption for Indistinguishability Obfuscation*, Cryptology ePrint Archive, Report 2015/581, 2015. [Online]. Available: https://eprint.iacr.org/2015/581.

[Can01] R. Canetti, "Universally Composable Security: A New Paradigm for Cryptographic Protocols", in *42nd IEEE Symposium on Foundations of Computer Science – FOCS 2001*, IEEE Computer Society, 2001, pp. 136–145.

[CGH04] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited", *Journal of the ACM*, vol. 51, no. 4, pp. 557–594, Jul. 2004.

[DFR+07] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, "A Tight High-Order Entropic Quantum Uncertainty Relation with Applications", in *Advances in Cryptology – CRYPTO 2007*, Springer Berlin Heidelberg, 2007, pp. 360–378.

[DGHM13] G. Demay, P. Gaži, M. Hirt, and U. Maurer, "Resource-Restricted Indifferentiability", in *Advances in Cryptology – EUROCRYPT 2013*, Springer Berlin Heidelberg, 2013, pp. 664–683.

[FM16] P. Farshim and A. Mittelbach, "Modeling Random Oracles Under Unpredictable Queries", in *Fast Software Encryption – FSE 2016*, Springer Berlin Heidelberg, 2016, pp. 453–473.

[MRH04] U. Maurer, R. Renner, and C. Holenstein, "Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology", in *Theory of Cryptography – TCC 2004*, Springer Berlin Heidelberg, 2004, pp. 21–39.

[Mau11] U. Maurer, "Constructive Cryptography–A New Paradigm for Security Definitions and Proofs", in *Theory of Security and Applications – TOSCA 2011*, Springer Berlin Heidelberg, 2011, pp. 33–56.

[Mau13] ——, "Conditional equivalence of random systems and indistinguishability proofs", in *2013 IEEE International Symposium on Information Theory*, IEEE, 2013, pp. 3150–3154.

[MR11] U. Maurer and R. Renner, "Abstract cryptography", in *In Innovations in Computer Science – ICS 2011*, Tsinghua University, 2011, pp. 1–21.

[MR16] ——, "From Indifferentiability to Constructive Cryptography (and Back)", in *Theory of Cryptography – TCC 2016*, Springer Berlin Heidelberg, 2016, pp. 3–24.

[Mit14] A. Mittelbach, "Salvaging Indifferentiability in a Multi-stage Setting", in *Advances in Cryptology – EUROCRYPT 2014*, Springer Berlin Heidelberg, 2014, pp. 603–621.

[RSS11] T. Ristenpart, H. Shacham, and T. Shrimpton, "Careful with Composition: Limitations of Indifferentiability and Universal Composability", in *Advances in Cryptology – EUROCRYPT 2011*, Springer Berlin Heidelberg, 2011, pp. 487–506.

[ST17] P. Soni and S. Tessaro, "Public-Seed Pseudorandom Permutations", in *Advances in Cryptology – EUROCRYPT 2017*, Springer International Publishing, 2017, pp. 412–441.

[Wul07] J. Wullschleger, "Oblivious-Transfer Amplification", in *Advances in Cryptology – EUROCRYPT 2007*, Springer Berlin Heidelberg, 2007, pp. 555–572.