Relaxing Full-Codebook Security: A Refined Analysis of Key-Length Extension Schemes[⋆]

Peter Gaži[⋆⋆], Jooyoung Lee[⋆⋆⋆], Yannick Seurin[†], John Steinberger[‡], and Stefano Tessaro[§]

April 27, 2015

Abstract. We revisit the security (as a pseudorandom permutation) of cascading-based constructions for block-cipher key-length extension. Previous works typically considered the extreme case where the adversary is given the *entire codebook* of the construction, the only complexity measure being the number q_e of queries to the underlying ideal block cipher, representing adversary's secret-key-independent computation. Here, we initiate a systematic study of the more natural case of an adversary restricted to adaptively learning a number q_c of plaintext/ciphertext pairs that is *less than the entire codebook.* For any such q_c, we aim to determine the highest number of block-cipher queries q_e the adversary can issue without being able to successfully distinguish the construction (under a secret key) from a random permutation.

More concretely, we show the following results for key-length extension schemes using a block cipher with n-bit blocks and κ-bit keys:

- Plain cascades of length $\ell = 2r + 1$ are secure whenever $q_c q_e^r \ll 2^{r(\kappa+n)}$, $q_c \ll 2^\kappa$ and $q_e \ll 2^{2\kappa}$. The bound for $r = 1$ also applies to two-key triple encryption (as used within Triple DES).
- The r-round XOR-cascade is secure as long as $q_c q_e^r \ll 2^{r(\kappa+n)}$, matching an attack by Gaži (CRYPTO 2013).
- We fully characterize the security of Gaži and Tessaro's two-call 2XOR construction (EUROCRYPT 2012) for all values of q_c, and note that the addition of a third whitening step strictly increases security for $2^{n/4} \le q_c \le 2^{3/4n}$. We also propose a variant of this construction *without* re-keying and achieving comparable security levels.

Keywords: block ciphers, key-length extension, provable security, ideal-cipher model

[⋆] This is the full version of the article submitted by the authors to the IACR and to Springer-Verlag in April 2015, which appears in the proceedings of FSE 2015.

[⋆⋆] IST Austria, E-mail: peter.gazi@ist.ac.at

[⋆⋆⋆] Sejong University, Seoul, Korea. E-mail: jlee05@sejong.ac.kr

[†] ANSSI, Paris, France. E-mail: yannick.seurin@m4x.org

[‡] Tsinghua University, P.R. China. E-mail: jpsteinb@gmail.com

[§] UC Santa Barbara. E-mail: tessaro@cs.ucsb.edu

1 Introduction

1.1 Block Ciphers and Key-Length Extension

Block ciphers (like DES [10] and AES [2]) are the workhorses of cryptography. Most importantly, they constitute the basic building block within several modes of operation for secret-key message encryption and authentication.

Formally, a block cipher with *key length* κ and *block length* n (often referred to as a (κ, n)-*block cipher*) is a family of efficiently computable (and invertible) permutations E_k on the set of n-bit strings indexed by a κ-bit key k. For example, $n = 64$ and $\kappa = 56$ for DES, and $n = 128$ and $\kappa \in \{128, 192, 256\}$ for AES.

Block-cipher security. Most applications assume and require that the underlying block cipher behaves as a *pseudorandom permutation* (PRP), i.e., under a random secret key, it cannot be efficiently distinguished from a uniformly random permutation. To capture this notion, the PRP-security level of a block cipher is defined as the complexity required to distinguish it from a random permutation with non-negligible advantage.

The security level of a block cipher E is inherently limited by its key length κ: Given very few plaintext-ciphertext pairs $(x_i, E_k(x_i))$, a generic brute-force attack can easily recover the secret key k with roughly 2^κ evaluations of E. This easily yields a PRP distinguishing attack with the same complexity. Clearly, this attack directly affects legacy designs with short keys, such as DES, for which 2^{56} is well within the boundaries of feasible computation.

Key-length extension and the ICM. Nonetheless, legacy designs often remain attractive in niche applications, like e.g. in the financial sector, where DES-based construction are used to encipher PIN numbers due to their short block length (as in the EMV standard [1]). In order to mitigate the effects of the above generic attacks, the well-known *key-length extension* (KLE) problem addresses the following question:

> *"Does there exist a construction* C *transforming any* (κ, n)*-block cipher* E *into a* (κ', n)*-block cipher* $\mathsf{C}[E]$ *(for* $\kappa' > \kappa$*), such that* $\mathsf{C}[E]$ *is secure against* generic *attackers (using* E *as a black-box) investing more than* 2^κ *effort?"*

Starting with the work of Killian and Rogaway on DESX [15], and followed by a series of subsequent works [5, 13, 14, 18, 12, 9], KLE has been formalized and studied in the *ideal cipher model* (ICM), where the underlying block cipher is modeled as an *ideal cipher*, i.e., E_k is an independent random permutation for every individual key k. Then, ICM PRP security of a KLE construction $\mathsf{C}[E]$ is captured by considering a random experiment where the attacker (also known as a *distinguisher*) issues two types of queries:

- **Block-cipher queries** to evaluate the block cipher $E_k(x)$ and $E_k^{-1}(y)$ for any k, x, and y chosen by the distinguisher.

- **Construction queries** to evaluate on a chosen n-bit input x either the KLE construction $\mathsf{C}[E]_{K'}$ with a uniformly random secret κ'-bit key K', or a uniform random permutation P independent of E. The respective inverses can also be evaluated.

The distinguisher's goal is to decide whether construction queries are answered by the construction or by P, and its power is measured in terms of the number $q_e \leq 2^{n+\kappa}$ of queries of the former type, and the number $q_c \leq 2^n$ of queries of the latter type. Security of C is measured in terms of which values of (q_c, q_e) do not allow distinguishing with non-negligible advantage.

Relaxing full-codebook security. So far, the security of KLE constructions (with the notable exception of the work of Killian and Rogaway [15]) has been analyzed in the *full-codebook regime*, i.e., where we allow $q_c = 2^n$, and then see how large q_e can be while still retaining pseudorandomness. However, there is often no rational reason to assume that $q_c = 2^n$. Not only this value is usually unreasonably large, but also, we can either easily restrict the number of block cipher evaluations on a certain secret key at the application level (by enforcing re-keying) *or* when using the KLE construction within a certain mode of operation, the security analysis of the latter may simply force security to only hold for smaller q_c anyway (e.g., $q_c \leq 2^{n/2}$ for CBC modes).

In this paper, we relax the unreasonably strong requirement of full-codebook security, and undertake the first in-depth investigation of the security of KLE constructions in the realistic scenario where $q_c \ll 2^n$.

1.2 Plain and Randomized Cascades

Before we turn to our contributions, let us first review previous works on KLE in the full-codebook regime $q_c = 2^n$. A summary of the attainable PRP security levels is given in Appendix A.

Cascading-based KLE. The most natural KLE approach is perhaps *cascading*, generalizing the idea behind triple DES. Formally, the cascade of length ℓ for a (κ, n)-block cipher E is the $(\ell \cdot \kappa, n)$-block cipher which takes an $\ell\kappa$-bit key $\mathsf{mk} = (k_1, \ldots, k_\ell) \in (\{0,1\}^\kappa)^\ell$ and encrypts a plaintext $x \in \{0,1\}^n$ by computing

$$y = \mathsf{CE}_{\mathsf{mk}}[E](x) = E_{k_\ell} \circ E_{k_{\ell-1}} \circ \cdots \circ E_{k_2} \circ E_{k_1}(x).$$

It is well known that the case $\ell = 2$ still allows for a 2^κ-query meet-in-the-middle attack (even though only a smaller distinguishing advantage is achievable for $q_e < 2^\kappa$ as shown by Aiello *et al.* [3]). For the case $r = 3$ (which generalizes 3DES), Bellare and Rogaway [5] first proved PRP security for $q_e \leq 2^{\kappa+n/2}$. This result was later generalized to arbitrary length ℓ by Gaži and Maurer [13]. Their bound on q_e was however far from tight, and was first improved by Lee [18], and a tight bound (matching an attack by Gaži [12]) was only recently given by Dai, Lee, Mennink, and Steinberger [9].

Randomized cascades. Another approach to key-length extension generalizes the DESX construction, using additional key material to randomize inputs and

Table 1. Overview of our results. Parameters q_c, q_e for which we prove security.

Construction	**Security**
XCE with r rounds	$q_c q_e^r \ll 2^{r(n+\kappa)}$ (Tight)
$\mathsf{2XOR}$	$q_e \ll \max\{2^{\kappa+n/2}, 2^{\kappa+n-\log(q_c)}\}$ (Tight)
$\mathsf{3XOR}$	$q_c \leq 2^{2/3n}$: $q_e \ll 2^{\kappa+\frac{4-\log(q_c)}{5}n}$ $q_c \in [2^{\frac{2}{3}n}, 2^{\frac{3}{4}n}]$: $q_e \ll 2^{\kappa+(2-2\log(q_c))n}$
$\mathsf{3XSK}$	$q_c \leq 2^{2/3n}$: $q_e \ll 2^{\kappa+\frac{4-\log(q_c)}{5}n}$
CE with $\ell = 2r+1$ rounds	$q_c q_e^r \ll 2^{r(\kappa+n)}$, $q_c \ll 2^{\kappa}$, $q_e \ll 2^{2\kappa}$
Two-key triple encryption	$q_c q_e \ll 2^{\kappa+n}$, $q_c \ll 2^{\kappa}$, $q_e \ll 2^{2\kappa}$

outputs of block-cipher calls. (This technique is often called *whitening*.) For example, the r-round XOR-cascade of a (κ, n)-block cipher E is the $(\kappa + (r+1)n, n)$-block cipher which, on input key (k, z) (where $z = (z_0, z_1, \ldots, z_r)$ consists of $(r+1)$ n-bit strings) and message x, returns

$$\mathsf{XCE}[E]((k,z),x) = \oplus_{z_r} \circ E_{\phi_r(k)} \circ \oplus_{z_{r-1}} \circ E_{\phi_{r-1}(k)} \circ \cdots \circ \oplus_{z_1} \circ E_{\phi_1(k)} \circ \oplus_{z_0}(x),$$

where $\oplus_z$ maps x' to $x' \oplus z$, and $\phi_1, \ldots, \phi_r$ are permutations on the κ-bit strings such that $\phi_i(k) \neq \phi_j(k)$ for all k and $i \neq j$. Security bounds for XOR-cascades in the full-codebook regime were proved by Lee [18] and by Gaži [12]. The latter work considered a variant without the last whitening step, and in combination with the result on key-alternating ciphers [8] led to tight bounds.

A simple variant of two-round XOR-cascades, called $\mathsf{2XOR}$, was studied by Gaži and Tessaro [14], where the third key z_2 is omitted, and $z_0 = z_1$. They prove PRP security for $q_e \leq 2^{\kappa+n/2}$, and that this security level is optimal (for $q_c = 2^n$) with respect to a large class of two-call constructions. We finally emphasize that the work by Killian and Rogaway [15] analyzing DESX (which is the case $r = 1$) is a notable exception to the above restriction to the full-domain regime, and exhibits a smooth security trade-off for any q_c and q_e as long as $q_c \cdot q_e \leq 2^{n+\kappa}$.

1.3 Our Contributions

While tight bounds are known in the full-codebook regime, the landscape is still mostly uncharted when moving to the case $q_c \ll 2^n$. This paper proves lower and upper bounds on the PRP security level of existing and new KLE constructions in the setting where $q_c \ll 2^n$. While a summary of our bounds is given in Table 1, we now discuss our contributions a bit more in detail.

We start with the randomized case:

- **Tight bounds for XOR cascades.** We provide *tight* bounds for XOR-cascades, matching an attack previously given by Gaži [12].
- **Characterizing $\mathsf{2XOR}$.** We complete the picture of the security of $\mathsf{2XOR}$ for all $q_c \leq 2^n$, showing that $q_e \leq 2^{\kappa+n/2}$ is tight when $q_c \in [2^{n/2}, 2^n]$,

and observing that otherwise $q_c \cdot q_e \leq 2^{\kappa+n}$ is necessary and sufficient for $q_c \leq 2^{n/2}$.

- **The 3XOR construction.** We show that adding the whitening key to the output of 2XOR yields a construction—that we name 3XOR—which is always at least as secure as 2XOR and strictly more secure for $2^{n/4} < q_c < 2^{3/4n}$.
- **A two-call construction with no re-keying.** We finally propose a variant of 3XOR (called 3XSK) where both block-cipher calls are with the *same* key, whereas the middle whitening key is a permutation of the original one. The security is comparable to that of 3XOR for $q_c \leq 2^{2/3n}$.

Our results also improve our picture with respect to plain cascading.

- **Odd-length plain cascades.** We prove that cascades of odd length $\ell = 2r + 1$ are secure whenever $q_c q_e^r \ll 2^{r(\kappa+n)}$, $q_c \ll 2^\kappa$, and $q_e \ll 2^{2\kappa}$. For κ and n satisfying $\kappa \geq \frac{rn}{r+1}$, this improves on the security bound of Dai *et al.* [9] when $q_c \leq 2^{\frac{rn}{r+1}}$. Moreover, when $\kappa \geq n$, this yields a tight bound (matching Gaži's attack [12]) for *all* parameters (for $\kappa \leq n$, the situation is more involved, see Section 5 for a complete discussion).
- **Two-key triple encryption.** We prove a similar bound for two-key triple encryption, where the first and third keys are identical, as in Triple DES.

Overview of our techniques. It turns out that the techniques behind our results are fairly general. We start by defining a general class of KLE constructions called *randomized KLE schemes*, that capture both plain cascades, XOR-cascades and others. Our core technical tool is then a lemma relating the security of a construction from this class to a particular cipher that can be derived from it, called a *sequential cipher*, also introduced here. Such ciphers constitute a generalization of key-alternating ciphers (or KACs, for short), studied in [6, 23, 16, 4, 17], and implement a block cipher by invoking a number of permutations in a sequential manner. Our lemma generalizes a previous result by Gaži [12], which only considered the case of KACs but neither our relaxation to randomized KLEs, nor the case without a full codebook.

To instantiate some of our bounds, we provide a generalized analysis of sequential ciphers, extending recent bounds by Chen and Steinberger [8].

1.4 Further Related Works

We note in passing that an orthogonal line of works devoted to cascade-like construction was initiated by Luby and Rackoff [19]. These works study *standard model* security amplification achieved by plain and randomized cascades, and in particular show how, when instantiated with a block cipher which is a weak PRP in the sense of the attacker achieving a large distinguishing advantage, these constructions reduce the best possible advantage with an increasing number of rounds. Increasingly tighter bounds have been given by Maurer and Tessaro [21], and by Tessaro [24]. An information-theoretic version of this question was also studied [25, 20].

2 Preliminaries

2.1 Basic Notation and Block Ciphers

In all the following, we fix integers $n, \kappa > 0$, and denote $N = 2^n$ and $K = 2^\kappa$. The set of all permutations on $\{0,1\}^n$ will be denoted $\mathcal{P}_n$. For a set T and an integer $\ell \geq 1$, $(T)_\ell$ denotes the set of all sequences that consist of ℓ distinct elements of T. For integers $1 \leq \ell \leq t$, we will write $(t)_\ell = t(t-1)\cdots(t-\ell+1)$. If $|T| = t$, then $(t)_\ell$ becomes the size of $(T)_\ell$.

A block cipher is a function family $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ such that for all $k \in \mathcal{K}$ the mapping $E(k, \cdot)$ is a permutation on $\{0,1\}^n$. We denote by $\mathsf{BC}(\mathcal{K}, n)$ the set of all such block ciphers, shortening to $\mathsf{BC}(\kappa, n)$ when $\mathcal{K} = \{0,1\}^\kappa$. In the ideal-cipher model, a block cipher E is chosen from $\mathsf{BC}(\kappa, n)$ uniformly at random and made available to the participants through oracle queries. It allows for two types of oracle queries $E(k,x)$ and $E^{-1}(k,y)$ for $x, y \in \{0,1\}^n$ and $k \in \{0,1\}^\kappa$.[1] The answer to an inverse query $E^{-1}(k,y)$ is $x \in \{0,1\}^n$ such that $E(k,x) = y$.

For a set $\mathcal{Q} = ((x_1, y_1), \ldots, (x_q, y_q)) \in (\{0,1\}^n \times \{0,1\}^n)^q$ and a permutation $P \in \mathcal{P}_n$, we say that P extends $\mathcal{Q}$, denoted $P \vdash \mathcal{Q}$, if $P(x_i) = y_i$ for $i = 1, \ldots, q$. The *domain* and the *range* of $\mathcal{Q}$ are defined as

$$\mathsf{Dom}(\mathcal{Q}) = \{x \in \{0,1\}^n : (x,y) \in \mathcal{Q}\}\ ,\ \mathsf{Rng}(\mathcal{Q}) = \{y \in \{0,1\}^n : (x,y) \in \mathcal{Q}\}$$

respectively. By an abuse of notation, we will sometimes denote $\mathcal{Q}$ the bijection from $\mathsf{Dom}(\mathcal{Q})$ to $\mathsf{Rng}(\mathcal{Q})$ such that $\mathcal{Q}(x_i) = y_i$ for $i = 1, \ldots, q$. Thus, for another set (bijection) $\mathcal{Q}' \in (\{0,1\}^n \times \{0,1\}^n)^{q'}$, we have

$$\mathsf{Dom}(\mathcal{Q}' \circ \mathcal{Q}) = \{x \in \{0,1\}^n : (x,y) \in \mathcal{Q} \wedge y \in \mathsf{Dom}(\mathcal{Q}')\}$$
$$\mathsf{Rng}(\mathcal{Q}' \circ \mathcal{Q}) = \{y \in \{0,1\}^n : (x,y) \in \mathcal{Q}' \wedge x \in \mathsf{Rng}(\mathcal{Q})\}$$

and similar definitions for the composition of more than two bijections. For a set $\mathcal{Q} = ((x_1, k_1, y_1), \ldots, (x_q, k_q, y_q)) \in (\{0,1\}^n \times \{0,1\}^\kappa \times \{0,1\}^n)^q$ and a block cipher $E \in \mathsf{BC}(\kappa, n)$, we say that E extends $\mathcal{Q}$, denoted $E \vdash \mathcal{Q}$, if $E(k_i, x_i) = y_i$ for $i = 1, \ldots, q$.

2.2 Indistinguishability in Idealized Models

In this paper, we consider block ciphers that are built (in a black-box way) on top of an existing primitive F. The primitive F is modeled as an ideal oracle (publicly accessible to the adversary), whose answers follow some probability distribution. Namely, we will consider two slightly different settings: the so-called *KLE-setting* where F will be the ideal cipher E; and the so-called *SC-setting*[2] where F will be a tuple of random permutations $\boldsymbol{P} = (P_1, \ldots, P_m)$. In both settings, we consider

[1] We interchangeably use both notations $E(k,x)$ and $E_k(x)$, and similarly $E^{-1}(k,y)$ and $E_k^{-1}(y)$.

[2] This refers to the notion of a *sequential cipher* defined in Section 3.1.

a construction C which encrypts a message $x \in \{0,1\}^n$ with some (master) key[3] $\mathsf{mk} \in \{0,1\}^{\kappa'}$ by making calls to F, and denote $\mathsf{C}[F]$ the resulting block cipher (hence $\mathsf{C}[F] \in \mathsf{BC}(\kappa', n)$, and $\mathsf{C}_{\mathsf{mk}}[F]$ is the permutation associated to key mk).

To define security, we consider an adversary (*a.k.a.* distinguisher) D which interacts with a pair of oracles that we denote generically (P, F). The goal of D is to distinguish whether it is interacting with $(\mathsf{C}_{\mathsf{mk}}[F], F)$ for some uniformly random key mk (a case we will informally refer to as the "real" world) or with (P, F) where P is a random n-bit permutation independent from F (the "ideal" world). Note that in both worlds the first oracle P is a permutation that can be queried in both directions. The distinguisher's advantage is defined as

$$\mathbf{Adv}_{\mathsf{C}}^{\mathrm{cca}}(\mathsf{D}) = \left| \Pr\left[\mathsf{D}^{\mathsf{C}_{\mathsf{mk}}[F],F} = 1\right] - \Pr\left[\mathsf{D}^{P,F} = 1\right] \right|$$

where the first probability is taken over the random choice of mk and the random answers of F, and the second probability is taken over the random choice of P and F. We refer to D's queries to its first and second oracle as *construction* and *primitive* queries, respectively. In the KLE-setting (SC-setting), the primitive queries are sometimes referred to more concretely as block-cipher queries (permutation queries), respectively.

In the KLE-setting, for $q_c, q_e \geq 0$ we define

$$\mathbf{Adv}_{\mathsf{C}}^{\mathrm{cca}}(q_c, q_e) = \max_{\mathsf{D}} \mathbf{Adv}_{\mathsf{C}}^{\mathrm{cca}}(\mathsf{D})$$

where the maximum is taken over all distinguishers making exactly q_c construction and q_e ideal-cipher queries. Similarly, in the SC-setting, for $q_c, q_p \geq 0$,

$$\mathbf{Adv}_{\mathsf{C}}^{\mathrm{cca}}(q_c, q_p) = \max_{\mathsf{D}} \mathbf{Adv}_{\mathsf{C}}^{\mathrm{cca}}(\mathsf{D})$$

where the maximum is taken over all distinguishers making exactly q_c construction queries and q_p permutation queries to *each* permutation oracle P_i.

In all the paper, we assume that the distinguisher is computationally unbounded, deterministic, and that it never makes redundant queries (these last two assumptions being *wlog*). In accordance with several recent works on the topic, we are using Patarin's H-coefficients technique [22] in some of our proofs. Our use of the H-coefficients technique will be self-contained, for a more detailed introduction to this method see for example [8].

3 From Randomized KLE Schemes to Sequential Ciphers

In this section we study the relationship of two general classes of constructions that we first define. On one hand, we consider *randomized KLE schemes* that

[3] We use the wording *master key* to emphasize that it will usually be used to derive sub-keys for calling the underlying block cipher. We also write $\mathsf{mk} = (k, z)$ for key-length extension schemes and $\mathsf{mk} = z$ for sequential ciphers (see Section 3.1).

generalize both cascades and XOR-cascades,[4] on the other hand we introduce *sequential ciphers* that are in turn a generalization of key-alternating ciphers (whose definition is also provided below). We show that every randomized KLE scheme induces a sequential cipher and the security properties of these two constructions are tightly connected.

3.1 Definitions

Randomized KLE. Let $n, \kappa > 0$ be some fixed parameters denoting the block- and key-length of the underlying block cipher, respectively. Fix additional parameters $\lambda, r, m > 0$. Let $(\phi_1, \ldots, \phi_m)$ be m permutations of $\{0,1\}^\kappa$ with the property that for any $k \in \{0,1\}^\kappa$, the values $(\phi_1(k), \ldots, \phi_m(k))$ are distinct. (Note that this imposes $m \leq 2^\kappa$.) Let $\sigma : \{1, \ldots, r\} \to \{1, \ldots, m\}$ be a surjective function.[5] For $i = 0, \ldots, r$, let

$$\rho^i : \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^n$$

be a function such that for each $z \in \{0,1\}^\lambda$, $\rho^i(z, \cdot)$ (also denoted $\rho^i_z(\cdot)$) is a permutation on $\{0,1\}^n$.[6]

A *randomized key-length extension scheme* R transforms a block cipher $E \in \mathsf{BC}(\kappa, n)$ into a new block cipher $\mathsf{R}[E] \in \mathsf{BC}(\kappa + \lambda, n)$ specified as follows: for a plaintext $x \in \{0,1\}^n$ and a key $(k, z) \in \{0,1\}^\kappa \times \{0,1\}^\lambda$, the ciphertext is defined as (see Figure 1)

$$\mathsf{R}[E]((k,z),x) = \rho^r_z \circ E_{k_{\sigma(r)}} \circ \rho^{r-1}_z \circ E_{k_{\sigma(r-1)}} \circ \cdots \circ E_{k_{\sigma(2)}} \circ \rho^1_z \circ E_{k_{\sigma(1)}} \circ \rho^0_z(x) \; .$$

where we simply write $(k_1, \ldots, k_m) = (\phi_1(k), \ldots, \phi_m(k))$. For a fixed key (k, z), we also denote $\mathsf{R}_{k,z}[E]$ the permutation $x \mapsto \mathsf{R}[E]((k,z),x)$.

Sequential Cipher. With the same primitives σ and $(\rho^0, \ldots, \rho^r)$, a *sequential cipher* S transforms a set of permutations $\boldsymbol{P} = (P_1, \ldots, P_m)$ into a block cipher $\mathsf{S}[\boldsymbol{P}] \in \mathsf{BC}(\lambda, n)$ specified as follows: for a plaintext $x \in \{0,1\}^n$ and a key $z \in \{0,1\}^\lambda$, the ciphertext is defined as (again see Figure 1)

$$\mathsf{S}[\boldsymbol{P}](z,x) = \rho^r_z \circ P_{\sigma(r)} \circ \rho^{r-1}_z \circ P_{\sigma(r-1)} \circ \cdots \circ P_{\sigma(2)} \circ \rho^1_z \circ P_{\sigma(1)} \circ \rho^0_z(x) \; .$$

For a fixed key z, we denote $\mathsf{S}_z[\boldsymbol{P}]$ the permutation $x \mapsto \mathsf{S}[\boldsymbol{P}](z,x)$.

[4] Our randomized KLE schemes also cover the notion of *sequential constructions* introduced in [12]. Since the latter are KLE schemes, they syntactically differ from the notion of a sequential cipher considered here.

[5] In case this causes confusion, r is the number of rounds, m is the number of distinct keys that are used to call the underlying block cipher, and σ specifies which key is used at each round.

[6] Though each ρ^i is syntactically a block cipher, we prefer to avoid this wording since in most of the paper the ρ^i's will be much simpler than E, the block cipher underlying the key-length extension scheme.

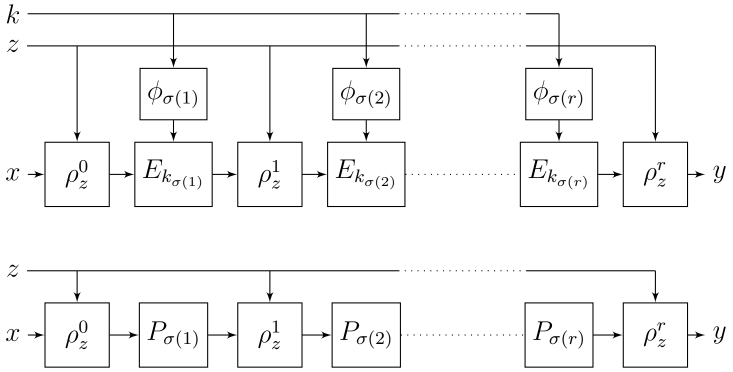

Fig. 1. The randomized key-length extension construction $\mathsf{R}[E]$ (top), and its induced sequential cipher $\overline{\mathsf{R}}[\boldsymbol{P}]$ (bottom).

3.2 Induced Sequential Ciphers

When the key k is fixed in some key-length extension scheme R, the resulting scheme can be regarded as a sequential cipher with key space $\{0,1\}^\lambda$ using independent random permutations $P_1, \dots, P_m$ in place of $E_{\phi_1(k)}, \dots, E_{\phi_m(k)}$ in the ideal cipher model. We formalize this remark as follows.

Definition 1. *Let* R *be a randomized key-length extension scheme defined as above. The* induced sequential cipher *of* R*, denoted* $\overline{\mathsf{R}}$*, is a sequential cipher which specifies a block cipher* $\overline{\mathsf{R}}[\boldsymbol{P}] \in \mathsf{BC}(\lambda, n)$ *from an* m*-tuple of permutations* $\boldsymbol{P} = (P_1, \dots, P_m)$ *of* $\{0,1\}^n$ *by replacing each call to* $E(\phi_i(k), \cdot)$*, resp.* $E^{-1}(\phi_i(k), \cdot)$ *when computing* $\mathsf{R}_{k,z}[E](x)$ *by a call to* $P_i(\cdot)$*, resp.* $P_i^{-1}(\cdot)$ *in the computation of* $\overline{\mathsf{R}}_z[\boldsymbol{P}](x)$*.*

Example 1. If we let σ be the identity, $\lambda = (r+1)n$ and $\rho^i(z, u) = u \oplus z_i$ for $i = 0, \dots, r$ where z is split as $z = (z_0, \dots, z_r) \in (\{0,1\}^n)^{r+1}$, then the resulting randomized KLE and sequential cipher constructions are called an *XOR-cascade scheme* and a *key-alternating cipher (KAC)*, respectively.

More formally, the r-round XOR-cascade construction XCE turns a block cipher $E \in \mathsf{BC}(\kappa, n)$ into a new block cipher $\mathsf{XCE}[E] \in \mathsf{BC}(\kappa + (r+1)n, n)$ as follows. Let $(\phi_1, \dots, \phi_r)$ be r permutations of $\{0,1\}^\kappa$ with the property that for any $k \in \{0,1\}^\kappa$, the values $(\phi_1(k), \dots, \phi_r(k))$ are distinct. Then for a plaintext $x \in \{0,1\}^n$ and a key $(k, z) \in \{0,1\}^\kappa \times (\{0,1\}^n)^{r+1}$ with $z = (z_0, \dots, z_r)$, the ciphertext is defined as (see also Figure 2):

$$\mathsf{XCE}[E]((k,z),x) = \oplus_{z_r} \circ E_{\phi_r(k)} \circ \oplus_{z_{r-1}} \circ E_{\phi_{r-1}(k)} \circ \cdots \circ \oplus_{z_1} \circ E_{\phi_1(k)} \circ \oplus_{z_0}(x),$$

where $\oplus_{z_i}$ denotes the mapping $x \mapsto x \oplus z_i$. Its induced sequential cipher $\overline{\mathsf{XCE}}$ is the key-alternating cipher (hence denoted KAC)

$$\overline{\mathsf{XCE}}[\boldsymbol{P}](z,x) = \mathsf{KAC}[\boldsymbol{P}](z,x) = \oplus_{z_r} \circ P_r \circ \oplus_{z_{r-1}} \circ P_{r-1} \circ \cdots \circ \oplus_{z_1} \circ P_1 \circ \oplus_{z_0}(x)\ .$$

A tight bound for the security of key-alternating ciphers was given in [8]. We show how to extend their approach to the more general case of sequential ciphers, as this will turn out to be useful in our later proofs. Due to space constraints, we present this extension in Appendix B.

Example 2. A more specialized case of the XOR-cascade scheme (i.e., taking $r = 1$) is the FX construction of [15] (the generic variant of DESX, attributed to Rivest) which turns a block cipher $E \in \mathsf{BC}(\kappa, n)$ into a block cipher $\mathsf{FX}[E] \in \mathsf{BC}(\kappa + 2n, n)$ defined as

$$\mathsf{FX}_{k,(z_0,z_1)}[E](x) = E_k(x \oplus z_0) \oplus z_1.$$

The resulting construction $\overline{\mathsf{FX}}$, for a permutation $P \in \mathcal{P}_n$, is

$$\overline{\mathsf{FX}}_{(z_0,z_1)}[P](x) = P(x \oplus z_0) \oplus z_1,$$

which is exactly the Even-Mansour cipher [11].

3.3 The Reduction

In this section we prove our main lemma that reduces the security of a randomized key-length extension scheme to the security of the corresponding induced sequential cipher. It can be seen as a generalization of [12, Theorem 2] to more general classes of constructions and as well to the setting where the number of construction queries q_c is arbitrary (rather than $q_c = 2^n$).

Lemma 1. *Let* R *be a randomized key-length extension scheme and let* $\overline{\mathsf{R}}$ *be its induced sequential cipher. Then for* $q_c, q_e, M > 0$*, one has*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{R}}(q_c, q_e) \leq \frac{mq_e}{KM} + \mathbf{Adv}^{\mathrm{cca}}_{\overline{\mathsf{R}}}(q_c, M).$$

Proof. Consider a distinguisher D interacting with (P, E), where E is an ideal cipher and P is either the construction $\mathsf{R}_{k,z}[E]$ for a uniformly random key $(k, z) \in \{0,1\}^\kappa \times \{0,1\}^\lambda$, or a random permutation independent from E. Following the H-coefficients technique [22, 8], we summarize all the information gathered by the distinguisher when interacting with the system (P, E) in the *raw query transcript* which is simply the ordered list of queries of D to its oracles together with their answers. From this raw query transcript we can build the *construction query transcript*

$$\mathcal{Q}_C = ((x_1, y_1), \ldots, (x_{q_c}, y_{q_c})),$$

where the i-th pair (x_i, y_i) indicates that the i-th query to the construction/random permutation oracle was either $P(x_i)$ with answer y_i or $P^{-1}(y_i)$ with answer y_i. Similarly, we can build the *ideal cipher query transcript*

$$\mathcal{Q}_E = ((u_1, k_1, v_1), \ldots, (u_{q_e}, k_{q_e}, v_{q_e})),$$

where the i-th triple (u_i, k_i, v_i) indicates that the i-th query to the ideal cipher was either $E(k_i, u_i)$ with answer v_i or $E^{-1}(k_i, v_i)$ with answer u_i. (Since the distinguisher is deterministic, the raw query transcript can unambiguously be reconstructed from the pair $(\mathcal{Q}_C, \mathcal{Q}_E)$.)

Moreover, in the real world, the key k (but not z) is given for free to D at the end of its queries, while in the ideal world (where no such key exists), a dummy key k is drawn uniformly at random and given to D. (This can only *increase* the distinguishing advantage since D can disregard this additional information.) This results in what we simply call the *transcript* $\tau = (\mathcal{Q}_C, \mathcal{Q}_E, k)$ of the attack. We will say that a transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_E, k)$ is *attainable* if there exists a permutation P and a block cipher E such that the interaction of D with (P, E) yields queries transcripts $(\mathcal{Q}_C, \mathcal{Q}_E)$ (said otherwise, the probability to obtain this transcript in the "ideal" world is non-zero). Finally, we let T_{re}, resp. T_{id} denote the probability distribution of the transcript τ induced by the real world, resp. the ideal world (note that these two probability distributions depend on the distinguisher). By extension, we use the same notation to denote a random variable distributed according to each distribution.

Let D be an optimal distinguisher making q_c construction queries and q_e ideal-cipher queries such that[7]

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{R}}(q_c, q_e) = \mathbf{Adv}^{\mathrm{cca}}_{\mathsf{R}}(\mathsf{D}) = \sum_{\tau \in \mathcal{T}_1} \Pr[T_{\mathrm{id}} = \tau] - \sum_{\tau \in \mathcal{T}_1} \Pr[T_{\mathrm{re}} = \tau]$$

and let $\mathcal{T}_1$ be the set of attainable transcripts $\tau = (\mathcal{Q}_C, \mathcal{Q}_E, k)$ such that the distinguisher outputs 1 when obtaining τ. Given an ideal-cipher queries transcript $\mathcal{Q}_E$, we also define the set of bad keys as

$$\mathsf{Bad}(\mathcal{Q}_E) = \{k \in \{0,1\}^\kappa : |\{(x, y) : (x, k, y) \in \mathcal{Q}_E\}| > M\}.$$

(Hence, a key k is bad if it appears strictly more than M times in $\mathcal{Q}_E$.) We say that an attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_E, k)$ is *bad* if $\phi_i(k) \in \mathsf{Bad}(\mathcal{Q}_E)$ for some $i = 1, \ldots, m$, and *good* otherwise. We denote resp. $\mathcal{T}_{\mathrm{bad}}$ and $\mathcal{T}_{\mathrm{good}}$ the sets of bad and good transcripts (which form a partition of the set of attainable transcripts $\mathcal{T}$). Then we have

$$\begin{aligned}\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{R}}(\mathsf{D}) &= \sum_{\tau \in \mathcal{T}_1} \Pr[T_{\mathrm{id}} = \tau] - \sum_{\tau \in \mathcal{T}_1} \Pr[T_{\mathrm{re}} = \tau] \\ &\leq \sum_{\tau \in \mathcal{T}_{\mathrm{bad}}} \Pr[T_{\mathrm{id}} = \tau] + \sum_{\tau \in \mathcal{T}_1 \cap \mathcal{T}_{\mathrm{good}}} \Pr[T_{\mathrm{id}} = \tau] - \sum_{\tau \in \mathcal{T}_1 \cap \mathcal{T}_{\mathrm{good}}} \Pr[T_{\mathrm{re}} = \tau] \quad (1)\end{aligned}$$

where the inequality follows from the fact that $\mathcal{T}_{\mathrm{good}}$ and $\mathcal{T}_{\mathrm{bad}}$ form a partition of the set of attainable transcripts $\mathcal{T}$. We upper bound each summand in turn.

Since in the ideal world the key k is drawn uniformly at random at the end of the interaction of the distinguisher with its oracles, we clearly can bound

[7] Without loss of generality, we can assume $\sum_{\tau \in \mathcal{T}_1} \Pr[T_{\mathrm{id}} = \tau] \geq \sum_{\tau \in \mathcal{T}_1} \Pr[T_{\mathrm{re}} = \tau]$ by slightly modifying D if necessary.

$\sum_{\tau\in\mathcal{T}_{\text{bad}}}\Pr[T_{\text{id}}=\tau]=\Pr[T_{\text{id}}\in\mathcal{T}_{\text{bad}}]$ as

$$\Pr[T_{\text{id}}\in\mathcal{T}_{\text{bad}}]\leq\sum_{i=1}^{m}\Pr[k\leftarrow_{\$}\{0,1\}^{\kappa}:\phi_i(k)\in\mathsf{Bad}(\mathcal{Q}_E)]\leq\frac{mq_e}{KM}\ , \qquad (2)$$

where the last inequality follows from the fact that each ϕ_i is a permutation (hence $\phi_i(k)$ is uniformly random) and that the size of $\mathsf{Bad}(\mathcal{Q}_E)$ is at most q_e/M by definition.

To upper bound the second term, we consider the following (probabilistic) distinguisher $\overline{\mathsf{D}}$ against construction $\overline{\mathsf{R}}$ (in the random permutation model), which uses D as a subroutine. $\overline{\mathsf{D}}$ has access to $m+1$ permutation oracles $(P_0,P_1,\ldots,P_m)$, where P_0 is either the construction $\overline{\mathsf{R}}_z[P_1,\ldots,P_m]$ for some random key $z\leftarrow_{\$}\{0,1\}^{\lambda}$, or a random permutation independent from $(P_1,\ldots,P_m)$. At the beginning of the experiment, $\overline{\mathsf{D}}$ draws a key $k\leftarrow_{\$}\{0,1\}^{\kappa}$ uniformly at random. Then, $\overline{\mathsf{D}}$ runs D and answers its queries as follows. First, it relays any construction query from D to its own construction oracle and relays back the corresponding answer to D. When D makes any ideal cipher query for some key $k'\notin\{\phi_1(k),\ldots\phi_m(k)\}$, $\overline{\mathsf{D}}$ simulates a perfectly random permutation associated with k'. If D makes an ideal cipher query for some key $\phi_i(k)$, $i=1,\ldots,m$, $\overline{\mathsf{D}}$ relays this query to permutation oracle P_i and forwards the corresponding answer to D. However, if D attempts to make more than M queries corresponding to some key $\phi_i(k)$, $i=1,\ldots,m$, then $\overline{\mathsf{D}}$ aborts and outputs 0. (Hence $\overline{\mathsf{D}}$ always makes at most M queries to each permutation oracle P_i, $i=1,\ldots,m$.) Otherwise, once D has finished its queries, $\overline{\mathsf{D}}$ forwards k to D (recall that we include k in the transcript) and outputs the same value as D. Clearly, when $\overline{\mathsf{D}}$ is interacting with $(P_0,P_1,\ldots,P_m)$, where P_0 is the construction $\overline{\mathsf{R}}_z[P_1,\ldots,P_m]$ then it is perfectly simulating the real world $(\mathsf{R}_{k,z}[E],E)$ to D, while when $\overline{\mathsf{D}}$ is interacting with $(P_0,P_1,\ldots,P_m)$ where P_0 is independent from $(P_1,\ldots,P_m)$, then it is perfectly simulating the ideal world (P,E) to D. Hence, the distinguishing advantage of $\overline{\mathsf{D}}$ is

$$\mathbf{Adv}^{\text{cca}}_{\overline{\mathsf{R}}}(\overline{\mathsf{D}})=\left|\sum_{\tau\in\mathcal{T}_1\cap\mathcal{T}_{\text{good}}}\Pr[T_{\text{re}}=\tau]-\sum_{\tau\in\mathcal{T}_1\cap\mathcal{T}_{\text{good}}}\Pr[T_{\text{id}}=\tau]\right|. \qquad (3)$$

Since $\overline{\mathsf{D}}$ makes at most q_c queries to its construction and at most M queries to each permutation oracle P_i, $i=1,\ldots,m$, and since in the information-theoretic setting the advantage of a probabilistic adversary cannot be larger than the one of the best deterministic adversary, one has

$$\mathbf{Adv}^{\text{cca}}_{\overline{\mathsf{R}}}(\overline{\mathsf{D}})\leq\mathbf{Adv}^{\text{cca}}_{\overline{\mathsf{R}}}(q_c,M). \qquad (4)$$

Combining (1), (2), (3), and (4), we obtain

$$\mathbf{Adv}^{\text{cca}}_{\mathsf{R}}(\mathsf{D})=\mathbf{Adv}^{\text{cca}}_{\mathsf{R}}(q_c,q_e)\leq\frac{mq_e}{KM}+\mathbf{Adv}^{\text{cca}}_{\overline{\mathsf{R}}}(q_c,M). \qquad \square$$

The following corollary can be easily obtained after optimization of M in Lemma 1 when one has a simple enough upper bound on $\mathbf{Adv}^{\text{cca}}_{\overline{\mathsf{R}}}(q_c,q_p)$.

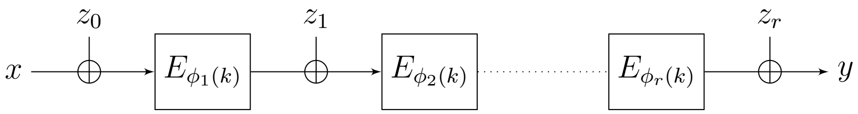

Fig. 2. The XOR-cascade key-length extension scheme $\mathsf{XCE}[E]$.

Corollary 1. *Let* R *be a randomized key-length extension scheme and let* $\overline{\mathsf{R}}$ *be its induced sequential cipher. Assume that*

$$\mathbf{Adv}^{\mathrm{cca}}_{\overline{\mathsf{R}}}(q_c, q_p) \le A + B\frac{q_c^{\alpha} q_p^{\beta}}{N^{\gamma}},$$

where $A, B, \alpha, \beta, \gamma$ *do not depend on* q_p*, and* $B \ge 1$*,* $\beta \ge 1$*. Then*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{R}}(q_c, q_e) \le A + mB(\beta+1)\left(\frac{q_c^{\alpha} q_e^{\beta}}{K^{\beta} N^{\gamma}}\right)^{\frac{1}{\beta+1}}.$$

4 Randomized Key-Length Extension Schemes

In this section, we derive security bounds for various randomized KLE schemes.

4.1 XOR-Cascades: Tight Bounds

As a first application, we complete the picture of the security of the XOR-cascade key-length extension scheme with independent whitening keys introduced in [12]. We derive a tight security bound for the setting with less than 2^n construction queries. Recall the definition of the r-round XOR-cascade construction XCE given in Section 3.2, Example 1.

Lemma 1 shows that the security of the r-round XOR-cascade construction is directly related to the security of the corresponding r-round key-alternating cipher KAC. It was observed in [12] to be related to the security of the $(r-1)$-round key-alternating cipher, but in hindsight this rather appears as an artifact of the setting $q_c = 2^n$.

Combining the result (6) on the security of KAC (following from [8] and given in Appendix B) with Lemma 1, we obtain that for any integer M such that $q_c + M \le N/2$,

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{XCE}}(q_c, q_e) \le \frac{rq_e}{KM} + 4(r+2)\left(\frac{rq_cM^r}{(r+2)N^r}\right)^{\frac{1}{r+1}}.$$

After the optimization of M (by equating the two summands), we arrive at the following theorem.

Theorem 1. *Consider the r-round XOR-cascade construction* XCE. *Then*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{XCE}}(q_c, q_e) \leq C_r \left(\frac{q_c q_e^r}{K^r N^r} \right)^{\frac{1}{2r+1}} ,$$

where C_r is a constant that depends only on r, namely

$$C_r = \left(2^{4r+3} \cdot r^{r+1}(r+2)^r\right)^{\frac{1}{2r+1}} \in \mathcal{O}(r).$$

In short, XOR-cascade encryption is secure as long as $q_c q_e^r$ is small compared to $2^{r(\kappa+n)}$. We note that this security bound is matched by a generic attack on sequential constructions given in [12, Theorem 3], since this attack can be easily generalized for arbitrary q_c as observed there.

4.2 2XOR: Tight Bounds

The construction $\mathsf{2XOR}$ was proposed by Gaži and Tessaro [14] to turn a block cipher $E \in \mathsf{BC}(\kappa, n)$ into a new block cipher $\mathsf{2XOR}[E] \in \mathsf{BC}(\kappa+n, n)$ defined as

$$\mathsf{2XOR}_{k,z}[E](x) = E_{\phi(k)}(E_k(x \oplus z) \oplus z) ,$$

where ϕ is any (fixed) permutation of $\{0,1\}^\kappa$ without fixed points. They showed the following result.

Theorem 2 ([14, Theorem 3]). *For any integer q_e,*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{2XOR}}(q_c = 2^n, q_e) \leq 4 \cdot \left(\frac{q_e}{2^{\kappa+n/2}} \right)^{\frac{2}{3}} .$$

We describe how to attack $\mathsf{2XOR}$ for any $1 \leq c \leq n/2$ using roughly 2^c construction queries and $2^{\kappa+n-c}$ block-cipher queries.

Theorem 3. *Let $1 \leq c \leq n/2$ and $1 \leq t \leq c$ be integers such that t is even. There exists a distinguisher D which makes at most $q_c = 2^{c+t/2}$ (forward) construction queries and $q_e = 2^{\kappa+n-c+t/2+1}$ ideal cipher queries, and which achieves*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{2XOR}}(\mathsf{D}) \geq 1 - 2^{\kappa+n-2^t(n-1)}.$$

In particular, for $c = n/2$ and $t = \lfloor \log_2(\kappa/n+1) \rfloor + 1$, its advantage is negligibly close to 1 (asymptotically in n), and its complexity is $q_c = \mathcal{O}(2^{n/2})$ and $q_e = \mathcal{O}(2^{\kappa+n/2})$ (for κ/n constant).

Proof. Consider the distinguisher D depicted in Figure 3 (we assume n to be even for simplicity). For its analysis, first note that for any $z \in \{0,1\}^n$, the size of the set V_z determined on line 10 is exactly 2^t, due to the choice of the sets X and U. When D interacts with $(\mathsf{2XOR}_{k,z}[E], E)$, it always outputs 1 since the check on line 11 succeeds for the real key (k, z). In the ideal world (P, E), we can upper-bound the probability that the distinguisher outputs 1 as follows: for each key (k, z), the values $\tilde{v}(k, u)$ and $\tilde{u}(k, x)$ for the 2^t pairs $(x, u) \in V_z$ are independent, so that the probability that the check on line 11 succeeds is exactly $\frac{1}{(2^n)_{2^t}} \leq 2^{-2^t(n-1)}$. By the union bound over the $2^{\kappa+n}$ pairs (k, z), the probability that D returns 1 is at most $2^{\kappa+n-2^t(n-1)}$. □

```
Distinguisher $\mathsf{D}^{S,E}$:                                 where $S \in \{\mathsf{2XOR}_{k,z}[E], P\}$
let $X := \{x'0^{n-c-t/2} : x' \in \{0,1\}^{c+t/2}\} \subseteq \{0,1\}^n$
let $U := \{0^{c-t/2}u' : u' \in \{0,1\}^{n-c+t/2}\} \subseteq \{0,1\}^n$
for all $x \in X$ do
    query $y(x) := S(x)$
for all $(k,x) \in \{0,1\}^\kappa \times X$ do
    query $\tilde{u}(k,x) := E^{-1}_{\phi(k)}(y(x))$
for all $(k,u) \in \{0,1\}^\kappa \times U$ do
    query $\tilde{v}(k,u) := E_k(u)$
for all $(k,z) \in \{0,1\}^\kappa \times \{0,1\}^n$ do
    let $V_z := \{(x,u) \in X \times U \mid x \oplus u = z\}$
    if $\forall (x,u) \in V_z : \tilde{v}(k,u) \oplus \tilde{u}(k,x) = z$ then
        return 1
return 0
```

Fig. 3. Distinguisher D for the proof of Theorem 3, attacking the construction $\mathsf{2XOR}$ and parametrized by c, t.

To illustrate that the tradeoff $q_c q_e \leq 2^{\kappa+n}$ imposed by the attack above is tight for $0 \leq \log_2(q_c) \leq n/2$, consider the sequential cipher $\overline{\mathsf{2XOR}}$ induced by $\mathsf{2XOR}$. By a trivial reduction (simulating its last, independent random permutation), one can show that $\overline{\mathsf{2XOR}}$ is at least as secure as the Even-Mansour cipher $\overline{\mathsf{FX}}$ described in Example 2 in Section 3.2. However, it follows from [11] that $\overline{\mathsf{FX}}$ is secure as long as $q_c q_p \leq 2^n$, which, via $\overline{\mathsf{2XOR}}$ and the application of Lemma 1, implies that $\mathsf{2XOR}$ is secure roughly as long as $q_c q_e \leq 2^{\kappa+n}$. This completes the picture for $\mathsf{2XOR}$ on the interval $0 \leq \log_2(q_c) \leq n/2$. For any $q_c \geq 2^{n/2}$, a tight bound for $\mathsf{2XOR}$ is $q_e = 2^{\kappa+n/2}$ as follows from Theorems 2 and 3, hence the security of $\mathsf{2XOR}$ is now understood for the full spectrum of parameters (q_c, q_e) (see Figure 5).

4.3 3XOR: Final Whitening Step Helps

It was also argued in [14] that the $\mathsf{2XOR}$ construction has optimal security within a large class of (so-called sequential) two-query constructions in the following sense: They give a generic attack on any construction from this class requiring roughly 2^n construction queries and $2^{\kappa+n/2}$ block-cipher queries, hence matching the security bound from Theorem 2. However, this only shows the optimality of the $\mathsf{2XOR}$ construction (and in particular, no need to add a final XOR step at its end) in the setting where $q_c = 2^n$ is assumed. As we show below, the situation changes as soon as we also consider lower values of q_c. In this general case, adding a third randomization step actually *does improve* security for some range of the parameters (q_c, q_e).

We define the $\mathsf{3XOR}$ construction similarly to the $\mathsf{2XOR}$ construction, but with a final whitening step (see Figure 4), i.e.,

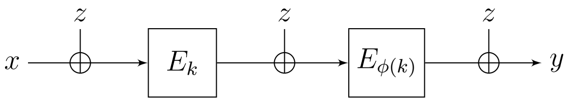

Fig. 4. The $\mathsf{3XOR}[E]$ key-length extension scheme.

$$\mathsf{3XOR}_{k,z}[E](x) = E_{\phi(k)}(E_k(x \oplus z) \oplus z) \oplus z \ .$$

Note that $\mathsf{3XOR}$ is simply the 2-round XCE construction with identical whitening keys in-between the block-cipher calls. The induced sequential cipher $\overline{\mathsf{3XOR}}$ is hence the 2-round Even-Mansour cipher with independent permutations and identical round keys:

$$\overline{\mathsf{3XOR}}_z[P_1, P_2](x) = P_2(P_1(x \oplus z) \oplus z) \oplus z \ .$$

The security of this construction was analyzed by Chen *et al.* [7]. We give their result as Theorem 8 in Appendix C. Combining it with Corollary 1, we obtain the following theorem for the security of the $\mathsf{3XOR}$ construction.

Theorem 4. *Assume that $n \geq 11$, $q_c \geq 9n$, $q_e \geq 9n$, and $2q_c + 2q_e \leq N$. Then the following upper bounds hold:*

(i) When $q_c \leq 2^{\frac{n}{4}}$, one has

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{3XOR}}(q_c, q_e) \leq 24 \left(\frac{q_c q_e}{KN}\right)^{\frac{1}{2}} .$$

(ii) When $2^{\frac{n}{4}} \leq q_c \leq 2^{\frac{2n}{3}}$, one has

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{3XOR}}(q_c, q_e) \leq \frac{6}{N} + 4 \times (13 + 9\sqrt{n}) \left(\frac{q_c^{\frac{1}{5}} q_e}{KN^{\frac{4}{5}}}\right)^{\frac{1}{2}} .$$

(iii) When $2^{\frac{2n}{3}} \leq q_c \leq 2^{\frac{3n}{4}}$, one has

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{3XOR}}(q_c, q_e) \leq \frac{6}{N} + 4 \times (13 + 9\sqrt{n}) \left(\frac{q_c^2 q_e}{KN^2}\right)^{\frac{1}{2}} .$$

(iv) When $q_c \geq 2^{\frac{3n}{4}}$, one has,

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{3XOR}}(q_c, q_e) \leq \frac{1}{eN} + 6n \left(\frac{q_e}{KN^{\frac{1}{2}}}\right)^{\frac{2}{3}} .$$

This security bound is qualitatively similar to the one of $\mathsf{2XOR}$ for $q_c \leq 2^{\frac{n}{4}}$ and $q_c \geq 2^{\frac{3n}{4}}$, but strictly better for $2^{\frac{n}{4}} \leq q_c \leq 2^{\frac{3n}{4}}$ (see Figure 5). Regarding the tightness of the bound, we note that the general attack against sequential

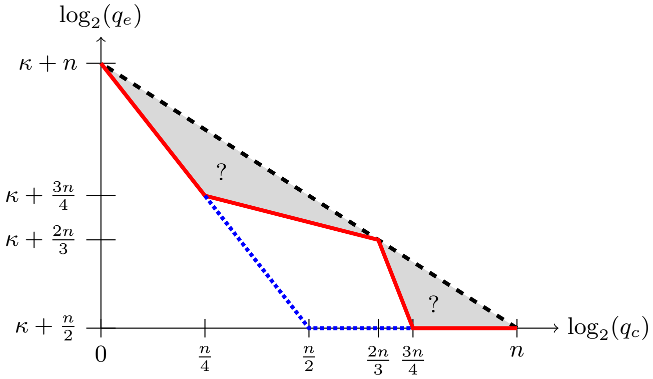

Fig. 5. The security of the 3XOR key-length extension scheme. All parameters below the (red) solid line are secure due to Theorem 4, while all parameters above the (black) dashed line are insecure due to the attack [12]. The status for parameters between these two lines remains unknown. The (blue) dotted line (which merges with the red solid line for $q_c \le 2^{\frac{n}{4}}$ and $q_c \ge 2^{\frac{3n}{4}}$) also indicates the (tight) security bound for 2XOR.

constructions given in [12, Theorem 3] applies to 3XOR, so that for any q_c, the construction is insecure for $q_e \approx 2^{\kappa+n-\frac{1}{2}\log_2 q_c}$. This matches the security bound for the special cases $q_c \approx 1$, $q_c \approx 2^{\frac{2n}{3}}$, and $q_c \approx 2^n$ (see Figure 5).

In conclusion, our results in Sections 4.2 and 4.3 show that 3XOR is *always* at least as secure 2XOR for all possible values of q_c, and strictly more secure for $2^{n/4} < q_c < 2^{3n/4}$.

4.4 3XSK: A 2-Call Construction without Rekeying

A drawback of the 3XOR construction is that the underlying block cipher E is called under two distinct keys. Since rekeying is typically a costly operation for a block cipher, it would be appealing to have a key-length extension construction providing the same level of security as 3XOR, but calling the underlying block cipher E with a single key. We describe such a construction in this section.

Let π be a linear orthomorphism of $\mathbb{F}_2^n$ (a permutation π of $\{0,1\}^n$ is an orthomorphism if $z \mapsto z \oplus \pi(z)$ is also a permutation).[8] We define the 3XSK (*3 XOR, single key*) construction which turns a block cipher $E \in \mathsf{BC}(\kappa, n)$ into a new block cipher $\mathsf{3XSK}[E] \in \mathsf{BC}(\kappa + n, n)$ as follows (see Figure 6):

$$\mathsf{3XSK}_{k,z}[E](x) = E_k(E_k(x \oplus z) \oplus \pi(z)) \oplus z.$$

The induced sequential cipher $\overline{\mathsf{3XSK}}$ is exactly the two-round Even-Mansour cipher with a single permutation and the sequence of round keys $(z, \pi(z), z)$,

$$\overline{\mathsf{3XSK}}_z[P](x) = P(P(x \oplus z) \oplus \pi(z)) \oplus z.$$

[8] For example, assuming n even, $\pi : (z_L, z_R) \mapsto (z_R, z_L \oplus z_R)$, where z_L and z_R are respectively the left and right halves of z, is an $\mathbb{F}_2$-linear orthomorphism.

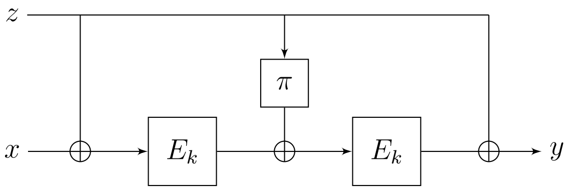

Fig. 6. The $\mathsf{3XSK}[E]$ key-length extension scheme.

Again, the security of this construction was studied by Chen *et al.* [7] and we restate their findings as Theorem 9 in Section C. Combining it with Corollary 1, we obtain the following theorem for the security of the 3XSK construction.

Theorem 5. *Assume that* $n \geq 9$*,* $q_c \geq 9n$*,* $q_e \geq 9n$*, and* $4q_c + 2q_e \leq N$*. Then the following upper bounds hold:*

(i) When $q_c \leq 2^{\frac{n}{3}}$*, one has*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{3XSK}}(q_c, q_p) \leq \frac{23}{N^{\frac{1}{3}}} + 32\left(\frac{q_c q_e}{KN}\right)^{\frac{1}{2}}.$$

(ii) When $q_c \geq 2^{\frac{n}{3}}$*, one has*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{3XSK}}(q_c, q_p) \leq \frac{10}{N} + (23 + 6\sqrt{n})\frac{q_c}{N^{\frac{2}{3}}} + 2 \times (39 + 9\sqrt{n})\left(\frac{q_e}{KN^{\frac{2}{3}}}\right)^{\frac{1}{2}}.$$

(Note that this bound becomes vacuous for $q_c \geq 2^{\frac{2n}{3}}$.)

This matches the security bound for 2XOR for $q_c < 2^{\frac{n}{3}}$, (and hence the lower bound proven for 3XOR in Section 4.3 for $q_c < 2^{\frac{n}{4}}$) while for $2^{\frac{n}{3}} \leq q_c \leq 2^{\frac{2n}{3}}$ it caps at $q_p \approx 2^{\kappa + \frac{2n}{3}}$ (hence it is slightly worse than the security lower bound of 3XOR in that case). The security for q_c larger than $2^{\frac{2n}{3}}$ remains unknown. Note that the attack given in [12] also applies to 3XSK exactly in the same way as to 3XOR, providing an upper bound on its security.

5 Plain Cascade Encryption

In this section, we give another application of Lemma 1, this time to analyze the security of plain cascade encryption in the setting where the number of construction queries is smaller than 2^n. Recall that the ℓ-round cascade encryption using a (κ, n)-block cipher E, denoted $\mathsf{CE}[E]$, takes an $\ell\kappa$-bit key $\mathsf{mk} = (k_1, \ldots, k_\ell) \in (\{0,1\}^\kappa)^\ell$ and encrypts a plaintext $x \in \{0,1\}^n$ by computing

$$y = \mathsf{CE}_{\mathsf{mk}}[E](x) = E_{k_\ell} \circ E_{k_{\ell-1}} \circ \cdots \circ E_{k_2} \circ E_{k_1}(x).$$

We focus on the security of CE for odd length $\ell = 2r + 1$ and our result is summarized in the following theorem.

Theorem 6. *Consider the ℓ-round cascade encryption* CE *where $\ell = 2r+1$ for some $r \geq 1$. Then, assuming $q_c \leq N/4$ and $q_e \leq KN/8$, one has*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{CE}}(q_c, q_e) \leq \frac{\ell^2}{K} + e^{-n} + r^2(r+1)\left(\frac{3nq_c}{K}\right)^{\frac{1}{2}} + \max\left\{A_r\left(\frac{q_c q_e^r}{K^r N^r}\right)^{\frac{1}{2r+1}}, B_r\left(\frac{nq_e}{K^2}\right)^{\frac{1}{3}}\right\},$$

where $A_r \in \mathcal{O}(r^2)$ and $B_r \in \mathcal{O}(r^{\frac{7}{3}})$ only depend on r, namely

$$A_r = 6r^2(r+1)\left(\frac{2^r}{r^{r+1}(r+1)^{r+1}}\right)^{\frac{1}{2r+1}}, \quad B_r = 6r^2(r+1)\left(\frac{3}{4r(r+1)}\right)^{\frac{1}{3}}.$$

Proof (sketch). From a high-level perspective, the proof consists of the following steps. First, we modify the cascade to use two *independent* ideal ciphers E and E' in an interleaving manner and show that this does not introduce a large distinguishing gap. Second, we need to assume that the block cipher E' used in the odd steps of the cascade is *good* in some well-defined sense and hence we show that the opposite is unlikely (over the randomness of E'). Third, we publish the complete function table of E' (but not the keys being used with it), thus arriving at a randomized KLE scheme of length r. Then we can apply Lemma 1 to reduce its security to the security of the induced sequential cipher. Finally, we analyze the latter directly, using an H-coefficient analysis inspired by [8] that employs the assumption that E' is good. The full proof discussing each of the individual steps in greater detail can be found in Appendix D. □

Discussion. In terms of the number of threshold queries, cascade encryption of length $\ell = 2r+1$ is hence secure when $q_c q_e^r \ll 2^{r(\kappa+n)}$, $q_c \ll 2^\kappa$, and $q_e \ll 2^{2\kappa}$ (asymptotically, ignoring constants). Our bound must be compared with the security result of Dai *et al.* [9], who considered the full-codebook regime $q_c = 2^n$. They showed that, for $\kappa \geq n/(r+1)$ (which is satisfied for virtually any real block cipher we know of), cascade encryption of length $\ell = 2r+1$ is secure when $q_e \ll 2^{\kappa+\frac{rn}{r+1}}$ (and, obviously, this also holds for any $q_c < 2^n$). Hence, our new bound improves on [9] when $q_c \leq 2^{\frac{rn}{r+1}}$, but only assuming $\kappa \geq \frac{rn}{r+1}$ since otherwise the condition $q_e \ll 2^{2\kappa}$ in our bound becomes more restrictive than Dai *et al.*'s one. This is depicted on Figure 7. We remark that our bound also applies to cascade encryption of length $2r+2$, since adding a round cannot decrease security.

Tightness. As observed in [12], the attack against cascades given there can be adjusted to provide a trade-off between block-cipher and construction queries. This results in an attack against plain cascade of length $\ell = 2r+1$ that achieves a constant distinguishing advantage as long as $q_c q_e^r \approx 2^{r(\kappa+n)}$ and $q_e \geq 2^\kappa q_c$ (again, ignoring constants). Note that the second condition only comes into play when $q_c \geq 2^{\frac{rn}{r+1}}$, in which case the attack requires $q_e \approx 2^{\kappa+\frac{rn}{r+1}}$ (instead of

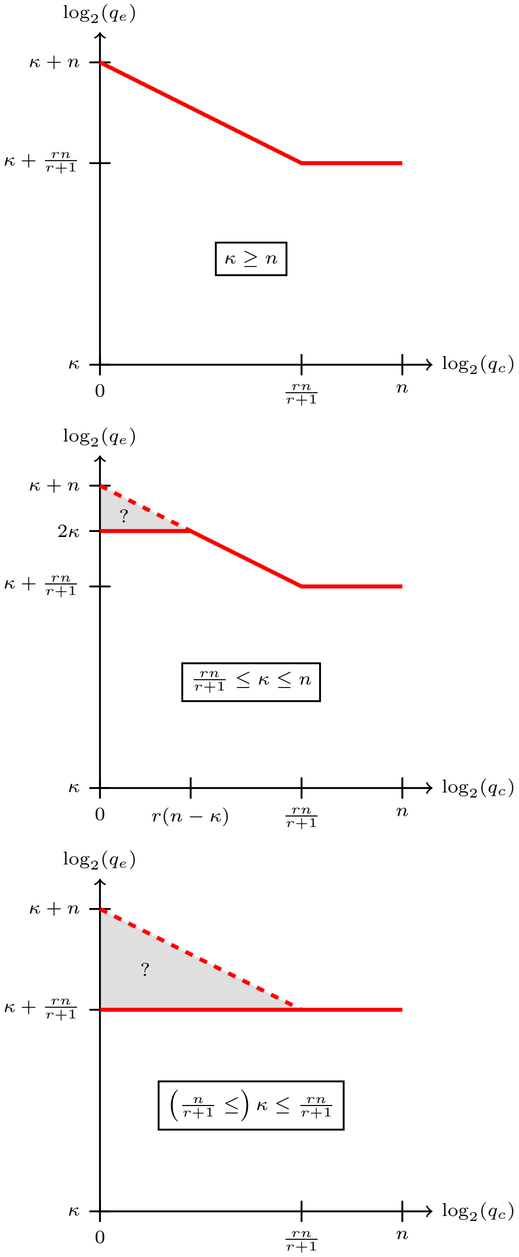

Fig. 7. The security of plain cascade encryption with $2r+1$ or $2r+2$ rounds, depending on κ and n. All parameters below the solid line are secure due either to Theorem 6 or the results of [9]. All parameters above the dashed line are insecure due to the attack of [12]. The status for parameters between these lines remains unknown.

$q_e \approx 2^{\kappa+n-\frac{1}{r}\log_2 q_c}$). Hence, this matches the bound of [9] for $q_c \geq 2^{\frac{rn}{r+1}}$. When $\kappa \geq n$, this also matches our own new bound for $q_c \leq 2^{\frac{rn}{r+1}}$, yielding a tight bound for all parameters. When $\frac{rn}{r+1} \leq \kappa \leq n$, the attack matches our new bound only for $q_c \geq 2^{r(n-\kappa)}$ since otherwise the security bound caps at $q_e \ll 2^{2\kappa} < 2^{\kappa+n-\frac{1}{r}\log_2 q_c}$. When $\kappa \leq \frac{rn}{r+1}$, there is a provable security gap between this attack and the bound of [9] for any $q_c \leq 2^{\frac{rn}{r+1}}$. This is also summarized on Figure 7. Again, all this applies to the case of cascade encryption of length $2r+2$ since Gaži's attack [12] was given for cascades of even length. Note that the case of 3DES ($\kappa = 56$, $n = 64$, and $r = 1$) corresponds to the middle graph.

Two-key Triple Encryption. Let TTE denote a variant of triple encryption where the first and the third keys are identical. So TTE accepts a 2κ-bit key $\mathsf{mk} = (k_1, k_2) \in (\{0,1\}^\kappa)^2$ and encrypts a plaintext $x \in \{0,1\}^n$ by computing $y = \mathsf{TTE}_{\mathsf{mk}}[E](x) = E_{k_1} \circ E_{k_2} \circ E_{k_1}(x)$. We prove the following result.

Theorem 7. *For the two-key triple encryption* TTE*, we have, assuming* $q_c \leq N/4$ *and* $q_e \leq KN/8$*,*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{TTE}}(q_c, q_e) \leq e^{-n} + 2\left(\frac{3nq_c}{K}\right)^{\frac{1}{2}} + 12\max\left\{\left(\frac{q_c q_e}{2KN}\right)^{\frac{1}{3}}, \left(\frac{3nq_e}{8K^2}\right)^{\frac{1}{3}}\right\}.$$

Proof (sketch). Similar to the analysis of cascade encryption in the proof of Theorem 6, we slightly modify the key-sampling process from **A** to **B**:

A: Choose $\mathsf{mk} \in (\{0,1\}^\kappa)^2$ uniformly at random.

B: Randomly partition $T_1 \cup T_2 = \{0,1\}^\kappa$ so that $|T_1| = |T_2|$, choose $z_1 \in T_1$ and $k_2 \in T_2$ uniformly at random, and then define $\mathsf{mk} = (z_1, k_2)$.

It is easy to show that these two processes have the same probability distribution. The rest of the proof follows exactly the same line of arguments as the proof of Theorem 6 for cascade encryption of length 3. □

Acknowledgment. Peter Gaži was partly funded by the European Research Council under an ERC Starting Grant (259668-PSPC).

Jooyoung Lee was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R1A1A2007488).

Yannick Seurin was partially supported by the French National Agency of Research through the BLOC project (contract ANR-11-INS-011).

John Steinberger was funded by National Basic Research Program of China Grant 2011CBA00300, 2011CBA00301, the National Natural Science Foundation of China Grant 61033001, 61361136003, and by the China Ministry of Education grant number 20121088050.

Stefano Tessaro was partially supported by NSF grant CNS-1423566.

References

[1] *EMV Integrated Circuit Card Specification for Payment Systems, Book 2: Security and Key Management, v.4.2.* June 2008.

[2] Advanced encryption standard (aes). National Institute of Standards and Technology (NIST), FIPS PUB 197, U.S. Department of Commerce, Nov. 2001.

[3] W. Aiello, M. Bellare, G. Di Crescenzo, and R. Venkatesan. Security amplification by composition: The case of doubly-iterated, ideal ciphers. In *CRYPTO'98*, volume 1462 of *LNCS*, pages 390–407. Springer, Aug. 1998.

[4] E. Andreeva, A. Bogdanov, Y. Dodis, B. Mennink, and J. P. Steinberger. On the indifferentiability of key-alternating ciphers. In *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 531–550. Springer, Aug. 2013.

[5] M. Bellare and P. Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 409–426. Springer, May / June 2006.

[6] A. Bogdanov, L. R. Knudsen, G. Leander, F.-X. Standaert, J. P. Steinberger, and E. Tischhauser. Key-alternating ciphers in a provable setting: Encryption using a small number of public permutations - (extended abstract). In *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 45–62. Springer, Apr. 2012.

[7] S. Chen, R. Lampe, J. Lee, Y. Seurin, and J. P. Steinberger. Minimizing the two-round Even-Mansour cipher. In *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 39–56. Springer, Aug. 2014.

[8] S. Chen and J. P. Steinberger. Tight security bounds for key-alternating ciphers. In *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 327–350. Springer, May 2014.

[9] Y. Dai, J. Lee, B. Mennink, and J. P. Steinberger. The security of multiple encryption in the ideal cipher model. In *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 20–38. Springer, Aug. 2014.

[10] Data encryption standard. National Bureau of Standards, NBS FIPS PUB 46, U.S. Department of Commerce, Jan. 1977.

[11] S. Even and Y. Mansour. A construction of a cipher from a single pseudorandom permutation. *Journal of Cryptology*, 10(3):151–162, 1997.

[12] P. Gaži. Plain versus randomized cascading-based key-length extension for block ciphers. In *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 551–570. Springer, Aug. 2013.

[13] P. Gaži and U. M. Maurer. Cascade encryption revisited. In *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 37–51. Springer, Dec. 2009.

[14] P. Gaži and S. Tessaro. Efficient and optimally secure key-length extension for block ciphers via randomized cascading. In *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 63–80. Springer, Apr. 2012.

[15] J. Kilian and P. Rogaway. How to protect DES against exhaustive key search (an analysis of DESX). *Journal of Cryptology*, 14(1):17–35, 2001.

[16] R. Lampe, J. Patarin, and Y. Seurin. An asymptotically tight security analysis of the iterated even-mansour cipher. In *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 278–295. Springer, Dec. 2012.

[17] R. Lampe and Y. Seurin. How to construct an ideal cipher from a small set of public permutations. In *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 444–463. Springer, Dec. 2013.

[18] J. Lee. Towards key-length extension with optimal security: Cascade encryption and xor-cascade encryption. In *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 405–425. Springer, May 2013.

[19] M. Luby and C. Rackoff. Pseudo-random Permutation Generators and Cryptographic Composition. In *Symposium on Theory of Computing - STOC '86*, pages 356–363. ACM, 1986.

[20] U. M. Maurer, K. Pietrzak, and R. Renner. Indistinguishability amplification. In *CRYPTO 2007*, volume 4622 of *LNCS*, pages 130–149. Springer, Aug. 2007.

[21] U. M. Maurer and S. Tessaro. Computational indistinguishability amplification: Tight product theorems for system composition. In *CRYPTO 2009*, volume 5677 of *LNCS*, pages 355–373. Springer, Aug. 2009.

[22] J. Patarin. The "coefficients H" technique (invited talk). In *SAC 2008*, volume 5381 of *LNCS*, pages 328–345. Springer, Aug. 2008.

[23] J. Steinberger. Improved security bounds for key-alternating ciphers via hellinger distance. Cryptology ePrint Archive, Report 2012/481, 2012. http://eprint.iacr.org/2012/481.

[24] S. Tessaro. Security amplification for the cascade of arbitrarily weak PRPs: Tight bounds via the interactive hardcore lemma. In *TCC 2011*, volume 6597 of *LNCS*, pages 37–54. Springer, Mar. 2011.

[25] S. Vaudenay. Adaptive-attack norm for decorrelation and super-pseudorandomness. In *SAC 1999*, volume 1758 of *LNCS*, pages 49–61. Springer, Aug. 1999.

A Overview of Previous Results

The following tables summarize the currently known best bounds for the full-codebook regime where $q_c = 2^n$. For a given ℓ (resp. r), ℓ' (resp. r') is the smallest even integer greater or equal to ℓ (resp. r).

ℓ-Round Plain Cascades

Ref.	**Max. value of** $\log(q_e)$	**Note**
[5]	$\kappa + \min\{n/2, \kappa/2\}$	$\ell = 3$
[13]	$\kappa + \min\{\kappa(\ell' - 2)/\ell', n/2\}$	
[18]	$\kappa + \min\{\kappa, n\} - 8n/\ell$	
[9]	$\kappa + \min\{\kappa(\ell' - 2)/2, n(\ell' - 2)/\ell'\}$	

r-Round Randomized Cascades

Ref.	**Max. value of** $\log(q_e)$	**Note**
[15]	$n + \kappa - \log(q_c)$	$r = 1$, FX
[14]	$\kappa + n/2$	$r = 2$, 2XOR
[18]	$\kappa + \min\{\kappa, n\} - 4n/r$	
[12]	$\kappa + \frac{r'-2}{r'}n$	

B Security Proof for a Sequential Cipher

Here we present an analysis of the security of a sequential cipher S that uses independent permutations in all steps (i.e., we assume that $m = r$ and σ is the identity function). The analysis given in this section is an extension of the result [8] with a slight modification in the definition of bad transcripts. We present it here since this modification will turn out to be useful in our analysis of the security of plain cascades in Section 5.

Under the assumption outlined above, and given keyed permutation families $(\rho^0, \dots, \rho^r)$, S transforms a tuple of permutations $\boldsymbol{P} = (P_1, \dots, P_r)$ into a block cipher $\mathsf{S}[\boldsymbol{P}] \in \mathsf{BC}(\lambda, n)$ specified as follows: for a plaintext $x \in \{0,1\}^n$ and a key $z \in \{0,1\}^\lambda$, the ciphertext is defined as

$$\mathsf{S}[\boldsymbol{P}](z, x) = \rho_z^r \circ P_r \circ \rho_z^{r-1} \circ P_{r-1} \circ \cdots \circ P_2 \circ \rho_z^1 \circ P_1 \circ \rho_z^0(x).$$

Fix some deterministic distinguisher D interacting with $(P_0, \boldsymbol{P})$ where P_0 is either the construction $\mathsf{S}_z[\boldsymbol{P}]$ for a uniformly random key $z \in \{0,1\}^\lambda$, or a random permutation independent from $\boldsymbol{P}$. Following the H-coefficients technique [22, 8], we summarize all the information gathered by the distinguisher when interacting with the system $(P_0, \boldsymbol{P})$ in what we call the *raw transcript* of the interaction, which is the ordered list of queries and answers received from the system (i, b, w, w'), where $i \in \{0, \dots, r\}$ names the permutation being queried, b is a bit indicating whether this is a forward or backward query, $w \in \{0,1\}^n$ is the actual value queried and w' the answer. We say that a transcript is *attainable* (with respect to some fixed distinguisher D) if there exists a tuple of permutations $(P_0, \dots, P_r) \in (\mathcal{P}_n)^{r+1}$ such that the interaction of D with $(P_0, \dots, P_r)$ yields this transcript (said otherwise, the probability to obtain this transcript in the "ideal" world is non-zero). In fact, an attainable transcript can be represented in a more convenient way that we will use in all the following. Namely, from the transcript we can build $r+1$ lists of directionless queries

$$\begin{aligned}
\mathcal{Q}_C &= ((x_1, y_1), \dots, (x_{q_c}, y_{q_c})) \\
\mathcal{Q}_{P_1} &= ((u_{1,1}, v_{1,1}), \dots, (u_{1,q_p}, v_{1,q_p})) \\
&\vdots \\
\mathcal{Q}_{P_r} &= ((u_{r,1}, v_{r,1}), \dots, (u_{r,q_p}, v_{r,q_p}))
\end{aligned}$$

as follows. For $j = 1, \dots, q_c$, let $(0, b, w, w')$ be the j-th query to P_0 in the transcript: if this was a forward query then we set $x_j = w$ and $y_j = w'$, otherwise we set $x_j = w'$ and $y_j = w$. Similarly, for each $i = 1, \dots, r$, and $j = 1, \dots, q_p$, let (i, b, w, w') be the j-th query to P_i in the transcript: if this was a forward query then we set $u_{i,j} = w$ and $v_{i,j} = w'$, otherwise we set $u_{i,j} = w'$ and $v_{i,j} = w$.

For attainable transcripts there is a one-to-one mapping between these two representations since the distinguisher is deterministic. Moreover, though we defined $\mathcal{Q}_C, \mathcal{Q}_{P_1}, \dots, \mathcal{Q}_{P_r}$ as ordered lists, the order is unimportant (our formalization keeps the natural order induced by the distinguisher).

Moreover, following [8], we will be generous with the distinguisher by providing it, at the end of its interaction, with the actual key z when it is interacting in the real world, or with a dummy key z selected uniformly at random when it is interacting in the ideal world. This cannot harm since the distinguisher is free to ignore this additional information. Hence, all in all a transcript τ is a tuple $(\mathcal{Q}_C, \mathcal{Q}_{P_1}, \dots, \mathcal{Q}_{P_r}, z)$. We will say that a transcript τ is attainable if $(\mathcal{Q}_C, \mathcal{Q}_{P_1}, \dots, \mathcal{Q}_{P_r})$ is attainable in the sense defined above.

Given an attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r}, z) \in \mathcal{T}$, we define the *contracted transcript* of τ, denoted $\tilde{\tau}$, where

$$\tilde{\tau} = (\tilde{\mathcal{Q}}_0, \tilde{\mathcal{Q}}_1, \ldots, \tilde{\mathcal{Q}}_r)$$

and $(x, y) \in \mathcal{Q}_C$ *iff* $(y, \rho_z^0(x)) \in \tilde{\mathcal{Q}}_0$ and $(u, v) \in \mathcal{Q}_{P_i}$ *iff* $(u, \rho_z^i(v)) \in \tilde{\mathcal{Q}}_i$ for $i = 1, \ldots, r$.

For $0 \leq i, j \leq r$, a *path* of type (i, j) is a tuple of points $(w_i, w_{i+1}, \ldots, w_j)$ such that $(w_\alpha, w_{\alpha+1}) \in \tilde{\mathcal{Q}}_\alpha$ for $\alpha = i, \ldots, j-1$, where the index increases cyclically modulo $r+1$. Let $\mathsf{P}(i, j)$ denote the number of paths of type (i, j) in $\tilde{\tau}$. Note that $\mathsf{P}(i, i+1) = q_p$ for $i = 0, \ldots, r-1$, and $\mathsf{P}(r, 0) = q_c$. For a constant $C \geq 2$, we will say that an attainable transcript τ is *bad* if either

$$\mathsf{P}(i, j) > \frac{C^{j-i-1} q_p^{j-i}}{N^{j-i-1}}$$

for some $i < j$, or

$$\mathsf{P}(i, j) > \frac{C^{r+j-i} q_c q_p^{r+j-i}}{N^{r+j-i}}$$

for some $i \geq j$.[9] Let $\mathcal{T}_{\mathrm{bad}}$ denote the set of bad transcripts. Assuming $q_c + q_p \leq N/2$ and using Lemma 1 in [8], we obtain the following upper bound.

$$\mathbf{Adv}_{\mathsf{S}}^{\mathrm{cca}}(q_c, q_p) \leq \frac{r 2^{r+1} C^r q_c q_p^r}{N^r} + \sum_{\tau \in \mathcal{T}_{\mathrm{bad}}} \Pr[T_{\mathrm{id}} = \tau]. \tag{5}$$

See Section B.1 for the proof (based on the same computation appearing in the proof of Theorem 1 in [8]).

Example 3. Consider the r-round key-alternating cipher KAC defined in Example 1 in Section 3.2. In the ideal world, the probability that a transcript satisfies $\mathsf{P}(i, j) > \frac{C^{j-i-1} q_p^{j-i}}{N^{j-i-1}}$ is upper bounded by $\frac{1}{C^{j-i-1}}$ if $1 \leq i+1 < j \leq r$, by Markov's inequality. With a similar analysis for the case $i \geq j$, we obtain

$$\sum_{\tau \in \mathcal{T}_{\mathrm{bad}}} \Pr[T_{\mathrm{id}} = \tau] = \sum_{h=1}^{r} \frac{r+1}{C^h} = \frac{(r+1)(C^r - 1)}{(C-1)C^r} \leq \frac{r+1}{C-1} \leq \frac{r+2}{C}$$

(assuming $r + 2 \leq C$) and hence

$$\mathbf{Adv}_{\mathsf{KAC}}^{\mathrm{cca}}(q_c, q_p) \leq \frac{r 2^{r+1} C^r q_c q_p^r}{N^r} + \frac{r+2}{C}.$$

Optimizing the constant C by solving $\frac{r 2^{r+1} C^r q_c q_p^r}{N^r} = \frac{r+2}{C}$, we have

$$\mathbf{Adv}_{\mathsf{KAC}}^{\mathrm{cca}}(q_c, q_p) \leq 4(r+2) \left(\frac{r q_c q_p^r}{(r+2) N^r} \right)^{\frac{1}{r+1}}. \tag{6}$$

[9] Compared to [8], we weakened the upper bounds on the number of paths of type (i, j) from $C q_p^{j-i} / N^{j-i-1}$ (resp. $C q_c q_p^{r+j-i} / N^{r+j-i}$) to $C^{j-i-1} q_p^{j-i} / N^{j-i-1}$ (resp. $C^{r+j-i} q_c q_p^{r+j-i} / N^{r+j-i}$).

B.1 Proof of Equation (5)

Fix a transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r}, z)$ that is not bad. Given a construction query (x_ℓ, y_ℓ), $\ell = 1, \ldots, q_c$, let

$$(w_i, w_{i+1}, \ldots, w_j)$$

be the longest path containing $w_0 (= \rho_z^0(x_\ell))$ and $w_r (= y_\ell)$ in the contracted transcript $\tilde{\tau}$, where $i \geq j$ and the index increases modulo $r+1$. So there is no $(w_{i-1}, w_i) \in \tilde{\mathcal{Q}}_i$ nor $(w_j, w_{j+1}) \in \tilde{\mathcal{Q}}_{j+1}$ for any w_{i-1} and w_{j+1}. In this case, we denote $\mathsf{L}(y_\ell) = i$ and $\mathsf{R}(x_\ell) = j$, and define the distance of the query (x_ℓ, y_ℓ) as $\mathsf{Dist}(x_\ell, y_\ell) = \mathsf{L}(y_\ell) - \mathsf{R}(x_\ell) (= i - j)$.

Let $\mathsf{Pr}(\ell)$ denote the conditional probability of $\mathsf{S}[\boldsymbol{P}](z, x_{\ell+1}) = y_{\ell+1}$ over the random choice of $\boldsymbol{P} = (P_1, \ldots, P_r)$ given that $\boldsymbol{P} \vdash (\mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r})$ and $\mathsf{S}[\boldsymbol{P}](z, x_i) = y_i$ for $i = 1, \ldots, \ell$. If $\mathsf{Dist}(x_{\ell+1}, y_{\ell+1}) = h \geq 1$, then by Lemma 1 in [8] and since $C \geq 2$ and $N \geq 2(q_c + q_p)$, we obtain

$$\begin{aligned}
\mathsf{Pr}(\ell) &\geq \frac{1}{N-\ell} - \frac{1}{N-\ell} \sum_{\sigma} \prod_{\alpha=1}^{|\sigma|} \frac{|\mathsf{P}(i_{\alpha-1}, i_\alpha)|}{N - \ell - |\mathsf{P}(i_\alpha - 1, i_\alpha)|} \\
&\geq \frac{1}{N-\ell} - \frac{1}{N-\ell} \sum_{\sigma} \prod_{\alpha=1}^{|\sigma|} \frac{C^{i_\alpha - i_{\alpha-1} - 1} q_p^{i_\alpha - i_{\alpha-1}} / N^{i_\alpha - i_{\alpha-1} - 1}}{N - \ell - q_p} \\
&= \frac{1}{N-\ell} - \frac{1}{N-\ell} \sum_{\sigma} \left(\frac{Cq_p}{N}\right)^h \left(\frac{N}{C(N - \ell - q_p)}\right)^{|\sigma|} \\
&= \frac{1}{N-\ell} - \frac{1}{N-\ell} \left(\frac{Cq_p}{N}\right)^h \sum_{s=1}^{h} \binom{h-1}{s-1} \left(\frac{N}{C(N - \ell - q_p)}\right)^s \\
&= \frac{1}{N-\ell} - \frac{1}{N-\ell} \left(\frac{Cq_p}{N}\right)^h \left(\frac{N}{C(N - \ell - q_p)}\right) \left(1 + \frac{N}{C(N - \ell - q_p)}\right)^{h-1} \\
&\geq \frac{1}{N-\ell} - \frac{1}{N-\ell} \left(\frac{Cq_p}{N}\right)^h \left(1 + \frac{N}{C(N - \ell - q_p)}\right)^h \\
&\geq \frac{1}{N-\ell} - \frac{1}{N-\ell} \left(\frac{2Cq_p}{N}\right)^h
\end{aligned}$$

where the sum is taken over all sequences $\sigma = (i_0, \ldots, i_s)$ with $\mathsf{R}_{\ell+1} = i_0 < \ldots < i_s = \mathsf{L}_{\ell+1}$, and where $|\sigma| = s$. For $h = 0, \ldots, r$, let

$$\mathcal{L}_h = \{\ell : \mathsf{Dist}(x_\ell, y_\ell) = h\} \subset \{1, \ldots, q_c\}.$$

Then sets $\mathcal{L}_0, \ldots, \mathcal{L}_r$ would partition the total set of indices $\{1, \ldots, q_c\}$. Since

$$|\mathcal{L}_h| \leq \frac{rq_c(Cq_p)^{r-h}}{N^{r-h}}$$

for $h \geq 1$, we have

$$\begin{aligned}\prod_{\ell+1\in\mathcal{L}_h} \frac{\mathsf{Pr}(\ell)}{1/(N-\ell)} &\geq \prod_{\ell+1\in\mathcal{L}_h}\left(1-\left(\frac{2Cq_p}{N}\right)^h\right)\\ &\geq 1-\frac{rq_c(Cq_p)^{r-h}}{N^{r-h}}\left(\frac{2Cq_p}{N}\right)^h\\ &= 1-\frac{rq_c(Cq_p)^r 2^h}{N^r}.\end{aligned}$$

For $h=0$, if $\frac{q_c(Cq_p)^r}{N^r} \geq 1$, then the above inequality trivially holds. Otherwise, we have $\mathcal{L}_0 = \emptyset$ since τ is not bad. Overall, we have

$$\frac{\Pr[T_{\mathrm{re}}=\tau]}{\Pr[T_{\mathrm{id}}=\tau]} = \prod_{\ell=0}^{q_c-1}\frac{\mathsf{Pr}(\ell)}{1/(N-\ell)} \geq 1-\sum_{h=0}^{r}\frac{rq_c(Cq_p)^r 2^h}{N^r} = 1-\frac{r(2^{r+1}-1)q_c(Cq_p)^r}{N^r}.$$

Therefore, for any distinguisher D making q_c construction queries and q_p permutation queries to each of the inner permutations, we have

$$\begin{aligned}\mathbf{Adv}(\mathsf{D}) &= \sum_{\tau\in\mathcal{T}_1}\left(\Pr[T_{\mathrm{id}}=\tau]-\Pr[T_{\mathrm{re}}=\tau]\right)\\ &= \sum_{\tau\in\mathcal{T}_1\setminus\mathcal{T}_{\mathrm{bad}}}\left(\Pr[T_{\mathrm{id}}=\tau]-\Pr[T_{\mathrm{re}}=\tau]\right)\\ &\qquad\qquad + \sum_{\tau\in\mathcal{T}_1\cap\mathcal{T}_{\mathrm{bad}}}\left(\Pr[T_{\mathrm{id}}=\tau]-\Pr[T_{\mathrm{re}}=\tau]\right)\\ &\leq \sum_{\tau\in\mathcal{T}_1\setminus\mathcal{T}_{\mathrm{bad}}}\left(\Pr[T_{\mathrm{id}}=\tau]-\Pr[T_{\mathrm{re}}=\tau]\right) + \sum_{\tau\in\mathcal{T}_{\mathrm{bad}}}\Pr[T_{\mathrm{id}}=\tau]\\ &\leq \sum_{\tau\in\mathcal{T}_1\setminus\mathcal{T}_{\mathrm{bad}}}\Pr[T_{\mathrm{id}}=\tau]\left(1-\frac{\Pr[T_{\mathrm{re}}=\tau]}{\Pr[T_{\mathrm{id}}=\tau]}\right) + \sum_{\tau\in\mathcal{T}_{\mathrm{bad}}}\Pr[T_{\mathrm{id}}=\tau]\\ &\leq \frac{r(2^{r+1}-1)q_c(Cq_p)^r}{N^r}\sum_{\tau\in\mathcal{T}_1\setminus\mathcal{T}_{\mathrm{bad}}}\Pr[T_{\mathrm{id}}=\tau] + \sum_{\tau\in\mathcal{T}_{\mathrm{bad}}}\Pr[T_{\mathrm{id}}=\tau]\\ &\leq \frac{r2^{r+1}q_c(Cq_p)^r}{N^r} + \sum_{\tau\in\mathcal{T}_{\mathrm{bad}}}\Pr[T_{\mathrm{id}}=\tau].\end{aligned}$$

C Some Previous Results on Sequential Ciphers

The following two results were proven in [7].

Theorem 8. *Consider the sequential cipher $\overline{\mathsf{3XOR}}$, i.e., the 2-round Even-Mansour cipher with independent permutations and identical round keys. Assume that $n \geq 11$, $q_c \geq 9n$, $q_p \geq 9n$, and $2q_c + 2q_p \leq N$. Then the following upper bounds hold:*

(i) When $q_c \le 2^{\frac{n}{4}}$, one has

$$\mathbf{Adv}^{\mathrm{cca}}_{\overline{\mathsf{3XOR}}}(q_c, q_p) \le \frac{6q_c q_p}{N}.$$

(ii) When $2^{\frac{n}{4}} \le q_c \le 2^{\frac{2n}{3}}$, one has

$$\mathbf{Adv}^{\mathrm{cca}}_{\overline{\mathsf{3XOR}}}(q_c, q_p) \le \frac{6}{N} + (13 + 9\sqrt{n})\frac{q_c^{\frac{1}{5}} q_p}{N^{\frac{4}{5}}}.$$

(iii) When $2^{\frac{2n}{3}} \le q_c \le 2^{\frac{3n}{4}}$, one has

$$\mathbf{Adv}^{\mathrm{cca}}_{\overline{\mathsf{3XOR}}}(q_c, q_p) \le \frac{6}{N} + (13 + 9\sqrt{n})\frac{q_c^2 q_p}{N^2}.$$

(iv) When $q_c \ge 2^{\frac{3n}{4}}$, one has,

$$\mathbf{Adv}^{\mathrm{cca}}_{\overline{\mathsf{3XOR}}}(q_c, q_p) \le \frac{1}{eN} + \frac{n q_p^2}{N}.$$

Theorem 9. *Consider the sequential cipher $\overline{\mathsf{3XSK}}$, i.e., the 2-round Even-Mansour cipher with a single permutation and round keys $(z, \pi(z), z)$. Assume that $n \ge 9$, $q_c \ge 9n$, $q_p \ge 9n$, and $4q_c + 2q_p \le N$. Then the following upper bounds hold:*

(i) When $q_c \le 2^{\frac{n}{3}}$, one has

$$\mathbf{Adv}^{\mathrm{cca}}_{\overline{\mathsf{3XSK}}}(q_c, q_p) \le \frac{23}{N^{\frac{1}{3}}} + \frac{16 q_c q_p}{N}.$$

(ii) When $q_c \ge 2^{\frac{n}{3}}$, one has

$$\mathbf{Adv}^{\mathrm{cca}}_{\overline{\mathsf{3XSK}}}(q_c, q_p) \le \frac{10}{N} + (23 + 6\sqrt{n})\frac{q_c}{N^{\frac{2}{3}}} + (39 + 9\sqrt{n})\frac{q_p}{N^{\frac{2}{3}}}.$$

D Proof of Theorem 6

Separating Block Ciphers. We begin by slightly modifying the key sampling process of CE. Consider the following two key-sampling processes.

A: Choose $\mathsf{mk} \in (\{0,1\}^\kappa)^\ell$ uniformly at random.

B: Randomly partition $T_1 \cup T_2 = \{0,1\}^\kappa$ so that $|T_1| = |T_2|$, choose $z = (z_0, \ldots, z_r) \in (T_1)^{r+1}$ and $k = (k_1, \ldots, k_r) \in (T_2)_r$ uniformly at random, and then define

$$\mathsf{mk} = (z_0, k_1, z_1, k_2, \ldots, k_r, z_r).$$

Then one can distinguish sampling processes $\mathbf{A}$ and $\mathbf{B}$ with advantage at most $\ell^2/2^\kappa$. We defer the proof of this claim to Appendix E.

In the ideal cipher model, each partition (T_0, T_1) produces two independent sets of block ciphers $\mathsf{BC}(T_0, n)$ and $\mathsf{BC}(T_1, n)$, each of which can be considered as $\mathsf{BC}(\kappa - 1, n)$. Therefore cascade encryption using key sampling processes $\mathbf{B}$ would have the same security as CE' that encrypts an n-bit message block x as

$$y = E'_{z_r} \circ E_{k_r} \circ \cdots \circ E'_{z_1} \circ E_{k_1} \circ E'_{z_0}(x)$$

where block ciphers E and E' are independently chosen from $\mathsf{BC}(\kappa - 1, n)$, and keys $z = (z_0, \ldots, z_r)$ and $k = (k_1, \ldots, k_r)$ are chosen uniformly at random from $\left(\{0,1\}^{\kappa-1}\right)^{r+1}$ and $\left(\{0,1\}^{\kappa-1}\right)_r$ respectively. Therefore we have

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{CE}}(q_c, q_e) \leq \frac{\ell^2}{2^\kappa} + \mathbf{Adv}^{\mathrm{cca}}_{\mathsf{CE}'}(q_c, q_e). \tag{7}$$

Choosing a Good Block Cipher E'. In order to analyze the security of CE', we require a certain property for E'. For A, $B \subset \{0,1\}^n$ and a fixed constant $C \geq 1$, let

$$\begin{aligned} \mathsf{Bad}(A, B, E') &= \left\{ z \in \{0,1\}^{\kappa-1} : |E'_z(A) \cap B| > \frac{C|A||B|}{N} \right\} \\ \mu(A, B, E') &= |\mathsf{Bad}(A, B, E')| \end{aligned} \tag{8}$$

where $E'_z(A) = \{E'_z(a) : a \in A\}$. We also fix a certain "threshold" number $M^* > 0$. We would like the maximum of $\mu(A, B, E')$ over the sets A and B such that $|A|, |B| \leq M^*$ to be small (compared to the total number of keys $K/2$) for most block ciphers $E' \in \mathsf{BC}(\kappa - 1, n)$.

Lemma 2. *Let $\mu(A, B, E')$ be defined as in (8). Then for any $\varepsilon > 0$,*

$$\Pr\left[E' \leftarrow_{\$} \mathsf{BC}(\kappa - 1, n) : \max_{|A|,|B| \leq M^*} \mu(A, B, E') > \left(\frac{1}{C} + \varepsilon\right)\frac{K}{2}\right] \leq e^{2nM^* - \varepsilon^2 K}.$$

Proof (of Lemma 2). Fix A, $B \subset \{0,1\}^n$ such that $|A|, |B| \leq M^*$ and fix a key $z \in \{0,1\}^{\kappa-1}$. Over a random choice of a block cipher $E' \in \mathsf{BC}(\kappa - 1, n)$, we define a random variable X_z where $X_z = 1$ if $|E'_z(A) \cap B| > \frac{C|A||B|}{N}$, and $X_z = 0$ otherwise. Since the expected value of $|E'_z(A) \cap B|$ is $\frac{|A||B|}{N}$, then by Markov's inequality, we have

$$\mathbb{E}(X_z) = \Pr\left[E' \leftarrow_{\$} \mathsf{BC}(\kappa - 1, n) : |E'_z(A) \cap B| > \frac{C|A||B|}{N}\right] \leq \frac{1}{C}.$$

Since random variables X_z, $z \in \{0,1\}^{\kappa-1}$, are independent and $\mu(A, B, E') = \sum_{z \in \{0,1\}^{\kappa-1}} X_z$, we can use Hoeffding's inequality to obtain

$$\Pr\left[\mu(A, B, E') > \left(\frac{1}{C} + \varepsilon\right)\frac{K}{2}\right] \leq e^{-\varepsilon^2 K}$$

for any real value $\varepsilon > 0$. Again, by using union bound over all possible pairs (A, B) of subsets and inequality

$$\left(\sum_{i=1}^{M^*} \binom{N}{i}\right)^2 \leq (N+1)^{2M^*} \leq e^{2nM^*}$$

we obtain the lemma. □

Fix parameters ε, M, $q_c > 0$ and $C \geq 1$ and let $M^* = \max\{M, q_c\}$. We will call a block cipher E' *good* if

$$\max_{|A|,|B| \leq M^*} \mu(A, B, E') \leq \left(\frac{1}{C} + \varepsilon\right) \frac{K}{2}.$$

Then we slightly modify CE' by having E' chosen uniformly at random from the set of good block ciphers. For the resulting encryption scheme, denoted CE'', we have

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{CE}'}(q_c, q_e) \leq e^{2nM^* - \varepsilon^2 K} + \mathbf{Adv}^{\mathrm{cca}}_{\mathsf{CE}''}(q_c, q_e) \tag{9}$$

by Lemma 2.

Publishing the Codebook of E'. In this step, we analyze the security of CE'' for a distinguisher given more power by allowing to make all possible queries to E'. This way, the block cipher E' becomes a permutation family (in the standard model). In order to analyze the security of CE'' using Lemma 1, we need to consider the corresponding sequential cipher $\overline{\mathsf{CE}''}$ that accepts a random key $z = (z_0, \ldots, z_r) \in (\{0,1\}^{\kappa-1})^{r+1}$ and encrypts an n-bit message block x as

$$y = E'_{z_r} \circ P_r \circ \cdots \circ E'_{z_1} \circ P_1 \circ E'_{z_0}(x)$$

where the key z is kept secret, $P_1, \ldots, P_r$ are modeled as independent random permutations on $\{0,1\}^n$ and E' is a good block cipher for which every evaluation has been revealed.

Security of the Sequential Cipher $\overline{\mathsf{CE}''}$. Consider a distinguisher $\overline{\mathsf{D}}$ for the induced cipher $\overline{\mathsf{CE}''}$ that makes exactly M queries to each of P_i, $i = 1, \ldots, r$, and q_c queries to P_0, where we denote P_0 the construction/random permutation oracle. For an attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r}, z) \in \mathcal{T}$ that $\overline{\mathsf{D}}$ obtains at the end of the interaction with the system of oracles, we will simply write $\mathcal{Q}_i = \mathcal{Q}_{P_i}$ for $i = 1, \ldots, r$ and define $\mathcal{Q}_0$, where $(x, y) \in \mathcal{Q}_C$ if and only if $(y, x) \in \mathcal{Q}_0$.

Fix $0 \leq i, j \leq r$ such that $j \not\equiv i + 1 \pmod{r+1}$. A key $z = (z_0, \ldots, z_r)$ is said to be *good of type* (i, j) if

$$z_{i+1} \notin \mathsf{Bad}\left(\mathsf{Rng}(\mathcal{Q}_{i+1}), \mathsf{Dom}(\mathcal{Q}_{i+2})\right)$$
$$z_{i+2} \notin \mathsf{Bad}\left(\mathsf{Rng}(\mathcal{Q}_{i+2} \circ E'_{z_{i+1}} \circ \mathcal{Q}_{i+1}), \mathsf{Dom}(\mathcal{Q}_{i+3})\right)$$

$$
\begin{aligned}
& z_{i+3} \notin \mathsf{Bad}\left(\mathsf{Rng}(\mathcal{Q}_{i+3} \circ E'_{z_{i+2}} \circ \mathcal{Q}_{i+2} \circ E'_{z_{i+1}} \circ \mathcal{Q}_{i+1}), \mathsf{Dom}(\mathcal{Q}_{i+4})\right) \\
& \qquad \vdots \\
& z_{j-1} \notin \mathsf{Bad}\left(\mathsf{Rng}(\mathcal{Q}_{j-1} \circ E'_{z_{j-2}} \circ \mathcal{Q}_{j-2} \circ \cdots \circ E'_{z_{i+1}} \circ \mathcal{Q}_{i+1}), \mathsf{Dom}(\mathcal{Q}_{j})\right)
\end{aligned}
$$

where the index increases modulo $r+1$. Let $\mathsf{P}(i,j)$ denote the number of paths of type (i,j) in the contracted transcript as defined in Appendix B.

First, note that if a key z is good of type (i,j), then we can easily upper-bound $\mathsf{P}(i,j)$. Namely, we have

$$
\mathsf{P}(i,j) \le \frac{C^{j-i-1} M^{j-i}}{N^{j-i-1}}
$$

for $i < j$, and

$$
\mathsf{P}(i,j) \le \frac{C^{j-i-1} q_c M^{j-i-1}}{N^{j-i-1}}
$$

for $i \ge j$, since when $j \not\equiv i+1 \pmod{r+1}$,

$$
\mathsf{P}(i,j) = \mathsf{Rng}(\mathcal{Q}_j \circ \rho_z^{j-1} \circ \mathcal{Q}_{j-1} \circ \cdots \circ \rho_z^{i+1} \circ \mathcal{Q}_{i+1}).
$$

Second, we establish a lower bound on the probability that a random key $z \in (\{0,1\}^{\kappa-1})^{r+1}$ is good of type (i,j). Since E' is a good block cipher and $|\mathsf{Rng}(\mathcal{Q}_i)|$, $|\mathsf{Dom}(\mathcal{Q}_{i+1})| \le M^*$, we have

$$
\left|\mathsf{Bad}\left(\mathsf{Rng}(\mathcal{Q}_i), \mathsf{Dom}(\mathcal{Q}_{i+1})\right)\right| \le \left(\frac{1}{C} + \varepsilon\right)\frac{K}{2}.
$$

So the probability that a random $z_i \in \{0,1\}^{\kappa-1}$ is in $\mathsf{Bad}\left(\mathsf{Rng}(\mathcal{Q}_i), \mathsf{Dom}(\mathcal{Q}_{i+1})\right)$ is upper bounded by $\frac{1}{C} + \varepsilon$. For each $\alpha = i+1, \ldots, j-2$ (increasing cyclically modulo $r+1$), suppose that

$$
\begin{aligned}
& z_{i+1} \notin \mathsf{Bad}\left(\mathsf{Rng}(\mathcal{Q}_{i+1}), \mathsf{Dom}(\mathcal{Q}_{i+2})\right) \\
& z_{i+2} \notin \mathsf{Bad}\left(\mathsf{Rng}(\mathcal{Q}_{i+2} \circ E'_{z_{i+1}} \circ \mathcal{Q}_{i+1}), \mathsf{Dom}(\mathcal{Q}_{i+3})\right) \\
& \qquad \vdots \\
& z_{\alpha-1} \notin \mathsf{Bad}\left(\mathsf{Rng}(\mathcal{Q}_{\alpha-1} \circ E'_{z_{\alpha-2}} \circ \mathcal{Q}_{\alpha-2} \circ \cdots \circ E'_{z_{i+1}} \circ \mathcal{Q}_{i+1}), \mathsf{Dom}(\mathcal{Q}_{j})\right)
\end{aligned}
$$

Given this condition, it follows that

$$
\left|\mathsf{Rng}(\mathcal{Q}_\alpha \circ E'_{z_{\alpha-1}} \circ \mathcal{Q}_{\alpha-1} \circ \cdots \circ E'_{z_{i+1}} \circ \mathcal{Q}_{i+1})\right| = \mathsf{P}(i,\alpha) \le \frac{C^\beta M^\beta M^*}{N^\beta} \le M^*
$$

assuming $CM/N \le 1$, where $\beta = \alpha - i$ if $i < \alpha$ and $\beta = r + \alpha + 1 - i$ otherwise.[10] Therefore the conditional probability that

$$
z_\alpha \in \mathsf{Bad}\left(\mathsf{Rng}(\mathcal{Q}_\alpha \circ E'_{z_{\alpha-1}} \circ \mathcal{Q}_{\alpha-1} \circ \cdots \circ E'_{z_i} \circ \mathcal{Q}_i), \mathsf{Dom}(\mathcal{Q}_{\alpha+1})\right)
$$

[10] If $CM/N > 1$, then the probability of obtaining bad transcripts in the ideal world becomes zero. So we don't need to consider this case.

for a random $z_\alpha \in \{0,1\}^{\kappa-1}$ is upper bounded by $\frac{1}{C} + \varepsilon$ again. Overall, the probability that a random key $z \in (\{0,1\}^{\kappa-1})^{r+1}$ is good of type (i,j) is at least $\left(1 - \left(\frac{1}{C} + \varepsilon\right)\right)^r$.

We now define a key $z \in (\{0,1\}^{\kappa-1})^{r+1}$ to be *bad* if it is not good of type (i,j) for some pair of (i,j). Accordingly, a transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r}, z) \in \mathcal{T}$ is said to be bad if z is a bad key. Then, for the set of bad transcripts $\mathcal{T}_{\text{bad}}$ we have

$$\begin{aligned}\sum_{\tau \in \mathcal{T}_{\text{bad}}} \Pr[T_{\text{id}} = \tau] &\leq r(r+1)\left(1 - \left(1 - \left(\frac{1}{C} + \varepsilon\right)\right)^r\right) \\ &\leq r(r+1)\left(1 - \left(1 - r\left(\frac{1}{C} + \varepsilon\right)\right)\right) \\ &\leq r^2(r+1)\left(\frac{1}{C} + \varepsilon\right).\end{aligned}$$

Therefore, by the bound (5) for sequential ciphers given in Appendix B, assuming $q_c + M \leq N/2$, we have

$$\mathbf{Adv}^{\text{cca}}_{\mathsf{CE}''}(q_c, M) \leq \frac{r2^{r+1}C^r q_c M^r}{N^r} + r^2(r+1)\left(\frac{1}{C} + \varepsilon\right). \tag{10}$$

Applying the Main Lemma. Finally, we apply Lemma 1 to CE'' along with (7), (9) and (10) to obtain, again assuming $q_c + M \leq N/2$,

$$\begin{aligned}\mathbf{Adv}^{\text{cca}}_{\mathsf{CE}}(q_c, q_e) &\leq \frac{\ell^2}{K} + \mathbf{Adv}^{\text{cca}}_{\mathsf{CE}'}(q_c, q_e) \\ &\leq \frac{\ell^2}{K} + e^{2nM^* - \varepsilon^2 K} + \mathbf{Adv}^{\text{cca}}_{\mathsf{CE}''}(q_c, q_e) \\ &\leq \frac{\ell^2}{K} + e^{2nM^* - \varepsilon^2 K} + \frac{rq_e}{MK} + \mathbf{Adv}^{\text{cca}}_{\mathsf{CE}''}(q_c, M) \\ &\leq \frac{\ell^2}{K} + e^{2nM^* - \varepsilon^2 K} + \frac{rq_e}{MK} + \frac{r2^{r+1}C^r q_c M^r}{N^r} \\ &\qquad + r^2(r+1)\left(\frac{1}{C} + \varepsilon\right).\end{aligned} \tag{11}$$

Optimizing Parameters. It remains to optimize parameters ε, M and C in Eq. (11). First, we set

$$M = \frac{Cq_e}{r(r+1)K},$$

so that

$$\frac{rq_e}{MK} = \frac{r^2(r+1)}{C}.$$

Next, if we set

$$\varepsilon = \left(\frac{3n(M+q_c)}{K}\right)^{\frac{1}{2}} = \left(\frac{3nCq_e}{r(r+1)K^2} + \frac{3nq_c}{K}\right)^{\frac{1}{2}} \leq \left(\frac{3nCq_e}{r(r+1)K^2}\right)^{\frac{1}{2}} + \left(\frac{3nq_c}{K}\right)^{\frac{1}{2}}$$

then we have

$$e^{2nM^*-\varepsilon^2 K} \leq e^{-n}$$

and hence

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{CE}}(q_c,q_e) \leq \frac{\ell^2}{K} + e^{-n} + \frac{2r^2(r+1)}{C} + \frac{2^{r+1}C^{2r}q_c q_e^r}{r^{r-1}(r+1)^r K^r N^r} + \\ + r^2(r+1)\left(\frac{3nCq_e}{r(r+1)K^2}\right)^{\frac{1}{2}} + r^2(r+1)\left(\frac{3nq_c}{K}\right)^{\frac{1}{2}} .$$

If we set

$$\frac{2r^2(r+1)}{C_1} = \frac{2^{r+1}C_1^{2r}q_c q_e^r}{r^{r-1}(r+1)^r K^r N^r}$$

then we obtain

$$C_1 = \left(\frac{r^{r+1}(r+1)^{r+1}K^r N^r}{2^r q_c q_e^r}\right)^{\frac{1}{2r+1}}$$

while by solving

$$\frac{2r^2(r+1)}{C_2} = r^2(r+1)\left(\frac{3nC_2 q_e}{r(r+1)K^2}\right)^{\frac{1}{2}}$$

we have

$$C_2 = \left(\frac{4r(r+1)K^2}{3nq_e}\right)^{\frac{1}{3}} .$$

So we put $C := \min\{C_1, C_2\}$ and also denote $D := \frac{\ell^2}{K} + e^{-n} + r^2(r+1)\left(\frac{3nq_c}{K}\right)^{\frac{1}{2}}$ to simplify the expressions. Then it follows that

$$\begin{aligned}\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{CE}}(q_c,q_e) &\leq D + 2r^2(r+1)\left(\max\left\{\frac{1}{C_1},\frac{1}{C_2}\right\} + \frac{1}{C_1} + \frac{1}{C_2}\right) \\ &\leq D + 6r^2(r+1)\max\left\{\frac{1}{C_1},\frac{1}{C_2}\right\} \\ &\leq D + 6r^2(r+1)\max\left\{\left(\frac{2^r q_c q_e^r}{r^{r+1}(r+1)^{r+1}K^r N^r}\right)^{\frac{1}{2r+1}}, \left(\frac{3nq_e}{4r(r+1)K^2}\right)^{\frac{1}{3}}\right\}\end{aligned}$$

as desired.

Finally, we need to verify that $M + q_c \leq N/2$ as required by (11). For this, it is sufficient to check that

$$\frac{24rq_e}{KN} \leq \frac{6r^2(r+1)}{C_1}, \tag{12}$$

which will imply

$$\frac{24rq_e}{KN} \leq \frac{6r^2(r+1)}{C} = \frac{6rq_e}{MK}$$

and hence $M \leq N/4$. Since also $q_c \leq N/4$ by assumption, we arrive at $M + q_c \leq N/2$ as needed. To prove (12), note that

$$
\begin{aligned}
(12) \iff \frac{24rq_e}{KN} &\leq 6r^2(r+1)\left(\frac{2^r q_c q_e^r}{r^{r+1}(r+1)^{r+1}K^rN^r}\right)^{\frac{1}{2r+1}} \\
\iff \frac{4q_e}{KN} &\leq r(r+1)\left(\frac{2^r q_c q_e^r}{r^{r+1}(r+1)^{r+1}K^rN^r}\right)^{\frac{1}{2r+1}} \\
\iff \frac{4^{2r+1}q_e^{2r+1}}{N^{2r+1}K^{2r+1}} &\leq r^{2r+1}(r+1)^{2r+1} \cdot \frac{2^r q_c q_e^r}{r^{r+1}(r+1)^{r+1}K^rN^r} \\
\iff \frac{2^{3r+2}q_e^{r+1}}{N^{r+1}K^{r+1}} &\leq r^r(r+1)^r q_c \\
\iff \left(\frac{8q_e}{NK}\right)^{r+1} &\leq 2r^r(r+1)^r q_c.
\end{aligned}
$$

This last inequality follows from the assumption that $q_e \leq KN/8$ (and the *wlog* assumption that $q_c \geq 1$).

E Distinguishing Key-Sampling Processes A and B

In order to analyze the distinguishing advantage of the two key-sampling processes, we introduce two intermediate processes **C1** and **C2** as follows.

C1: Choose $\mathsf{mk} \in (\{0,1\}^\kappa)_\ell$ uniformly at random.

C2: Randomly partition $T_1 \cup T_2 = I_\kappa$ so that $|T_1| = |T_2|$, choose $z = (z_0, \ldots, z_r) \in (T_1)_{r+1}$ and $k = (k_1, \ldots, k_r) \in (T_2)_r$ uniformly at random, and then define

$$\mathsf{mk} = (z_0, k_1, z_1, k_2, \ldots, k_r, z_r).$$

Note that one can distinguish the sampling processes **A** and **C1** with advantage at most

$$\binom{\ell}{2}\frac{1}{2^\kappa} \leq \frac{\ell^2}{2^{\kappa+1}} \; , \tag{13}$$

and the sampling processes **C2** and **B** with advantage at most

$$\binom{r+1}{2}\frac{1}{2^\kappa} \leq \frac{(r+1)^2}{2^{\kappa+1}} \leq \frac{\ell^2}{2^{\kappa+1}} \; . \tag{14}$$

On the other hand, the sampling processes **C1** and **C2** have exactly the same probability distribution. To see this, fix a key $\mathsf{mk} = (z_0, k_1, z_1, k_2, \ldots, k_r, z_r) \in (\{0,1\}^\kappa)_\ell$. Then the number of partitions (T_1, T_2) such that $\{z_0, z_1, \ldots, z_r\} \subset T_1$ and $\{k_1, \ldots, k_r\} \subset T_2$ is

$$\binom{K-\ell}{\frac{K}{2}-r}.$$

For each of such partitions (T_1, T_2), the key-sampling process **C2** chooses $z = (z_0, \ldots, z_r)$ and $k = (k_1, \ldots, k_r)$ from T_1 and T_2, respectively, with probability

$$\frac{1}{\left(\frac{K}{2}\right)_r \cdot \left(\frac{K}{2}\right)_{r+1}}.$$

So the probability that **C2** chooses z and k is

$$\frac{\binom{K-\ell}{\frac{K}{2}-r}}{\binom{K}{\frac{K}{2}}} \cdot \frac{1}{\left(\frac{K}{2}\right)_r \cdot \left(\frac{K}{2}\right)_{r+1}} = \frac{1}{(K)_\ell}$$

which is the same as the probability that the key-sampling process **C1** chooses mk.

Therefore, (13) and (14) together imply that one can distinguish the sampling processes **A** and **B** with advantage at most $\ell^2/2^\kappa$.