Plain versus Randomized Cascading-Based Key-Length Extension for Block Ciphers

Peter Gaži

ETH Zürich, Switzerland
Department of Computer Science
peter.gazi@inf.ethz.ch

Abstract. The security of cascading-based key-length extending constructions for block ciphers in the ideal-cipher model has so far received considerable attention. Triple encryption was investigated in [20,9], longer cascades were considered in [15] and a construction with comparable security as triple encryption requiring only 2 block-cipher calls, so-called 2-XOR-cascade, was proposed and analyzed in [17].

In this paper we put these results into perspective by completing the picture of the investigated landscape in various ways. We give the following attacks and security lower bounds for constructions using a block cipher with key length κ and block length n:

- For the plain cascade of odd (resp. even) length ℓ we present a generic attack requiring roughly $2^{\kappa+\frac{\ell-1}{\ell+1}n}$ (resp. $2^{\kappa+\frac{\ell-2}{\ell}n}$) queries. This is a generalization of both the meet-in-the-middle attack on double encryption and the best known attack on triple cascade given in [20].
- For the general case of XOR-cascade of odd (resp. even) length ℓ we prove security up to $2^{\kappa+\frac{\ell-1}{\ell+1}n}$ (resp. $2^{\kappa+\frac{\ell-2}{\ell}n}$) queries and also an improved bound $2^{\kappa+\frac{\ell-1}{\ell}n}$ for the special case $\ell \in \{3,4\}$. This is achieved by relating the problem to an independent line of work on the security of key-alternating ciphers in the random-permutation model.
- Finally, for a natural class of *sequential* constructions where block-cipher encryptions are interleaved with key-dependent permutations, we show a generic attack requiring roughly $2^{\kappa+\frac{\ell-1}{\ell}n}$ queries. Since XOR-cascades are sequential, this proves tightness of our above result for XOR-cascades of length $\ell \in \{3,4\}$ as well as their optimal security within the class of sequential constructions.

These results suggest that XOR-cascades achieve a better security/efficiency trade-off than plain cascades and should be preferred.

Keywords: Provable security, block ciphers, key-length extension, ideal-cipher model, cascade, XOR-cascade.

1 Introduction

1.1 Block Ciphers and the Key-Length Extension Problem

It is beyond question that block ciphers play a pivotal role in cryptographic practice, being the basic building block for most constructions in the realm of symmetric cryptography. The first standardized block cipher achieving huge popularity and wide-spread use was DES [1], nowadays being replaced by the current standard AES [4].

Formally, a block cipher with keyspace $\{0,1\}^\kappa$ and message space $\{0,1\}^n$ is simply a family of efficiently computable (and invertible) permutations E_k on the set of n-bit strings indexed by a κ-bit key k, which is often emphasized by referring to it as a (κ, n)-block cipher. For example, $n = 64$ and $\kappa = 56$ for DES, and $n = 128$ and $\kappa \in \{128, 192, 256\}$ for AES.

In most applications that employ a block cipher as its underlying primitive, it is assumed (and required) that it behaves as a *pseudorandom permutation* (PRP), i.e., if used with 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.

Key-Length Extension. The key length κ is a crucial security parameter of every block cipher E. An attacker, given some plaintext-ciphertext pairs, can easily identify the secret key being used by a brute-force attack if he is capable of performing roughly 2^{κ} evaluations of E. This key-recovery attack can be also transformed into a PRP distinguishing attack, implying that the bound of 2^{κ} evaluations limits the PRP security of every block cipher. This represents a problem for existing block ciphers with small key length κ for which 2^{κ} operations can no longer be considered beyond the available computational power of a potential attacker.

A prominent example of such a design is the former standard DES, which however, apart from its insufficient key size, is believed to contain no significant structural weaknesses. It also remains attractive thanks to its short block length which allows enciphering short inputs and explains the wide-spread use of DES-based constructions in the financial industry even today (see e.g. [6] for the EMV standard).

Due to the above reasons, there exists a practical demand for constructions transforming any (κ, n)-block cipher E into a (κ', n)-block cipher C^{E} while increasing both the key length (i.e., $\kappa' > \kappa$) and the generic security achieved (i.e., the PRP security of C^{E} should be significantly higher than 2^{κ} assuming that E itself contains no non-generic weaknesses). This is known as the *key-length extension problem* for block ciphers and in this paper we contribute to the understanding and analysis of several cascading-based constructions addressing this problem. Note that even though the case of DES constituted the initial motivation for the study of key-length extension, we focus on generic constructions that are applicable to any block cipher, making our results attractive also from a theoretic perspective.

Ideal-Cipher Model. To assess the security level achieved by the key-length extension constructions themselves, we assume the absence of any weaknesses of the underlying block cipher by modelling it as the *ideal* block cipher $\mathbf{E}$ providing an independent uniformly random permutation for each key. We consider a distinguisher $\mathbf{D}$ that is allowed to issue two types of queries:

- *block-cipher queries* to evaluate the block cipher $\mathbf{E}$ under any key and on any input block (both in the encryption and the decryption direction).
- *construction queries* to evaluate either the key-length extending construction $\mathsf{C}^{\mathbf{E}}_{K'}$ used with the block cipher $\mathbf{E}$ and a uniformly random secret κ'-bit key K'; or a uniform random permutation $\mathbf{P}$ independent of $\mathbf{E}$ (again, both query directions are allowed).

Hence, the distinguisher is either given to interact with the combined system $(\mathbf{E}, \mathsf{C}^{\mathbf{E}}_{K'})$ or with $(\mathbf{E}, \mathbf{P})$ and its goal is to decide which of these two situations has occurred. Its complexity is determined solely by the sum of its queries of both types, leading to results of information-theoretic nature. Note that the security of *any* key-length extension construction in this model can be upper-bounded by $2^{\kappa+n}$ which corresponds to the trivial attack asking all possible block cipher and construction queries. This model has already been employed numerous times to analyze the security of key-length extending constructions, e.g. in [18,9,15,17].

1.2 Plain and Randomized Cascades

Arguably the most natural way to approach the key-length extension problem is to simply apply the block cipher several times using an independent key at each step – an approach known as *cascading*. Its security has been a subject of extensive study in various models, including the information-theoretic ideal-cipher model described above. It is well known that a cascade of length two does not substantially increase security due to the meet-in-the-middle attack [11], even though a security increase in terms of distinguishing advantage is achieved for low attack complexities, as shown in [7]. This makes triple encryption the shortest cascade with a potential for significant security gain, resulting into its widespread usage as the *Triple-DES* (3DES) standard [2,3,5]. Given keys $k_1, k_2, k_3 \in \{0,1\}^{56}$, 3DES encrypts a 64-bit message m as

$$\mathrm{3DES}_{k_1,k_2,k_3}(m) = \mathrm{DES}_{k_3}(\mathrm{DES}_{k_2}(\mathrm{DES}_{k_1}(m))) \ .$$

The security of 3DES (and its variant using decryption in the second step of the cascade) was formally studied by Bellare and Rogaway [9], showing its security up to roughly $2^{\kappa+\min\{n,\kappa\}/2}$ queries when DES is replaced by an ideal block cipher. Subsequently Gaži and Maurer [15] showed that the security increases further with the length of the cascade for block ciphers where $\kappa \leq n$, approaching roughly $2^{\min\left\{\frac{2\ell\kappa}{\ell+1},\kappa+\frac{n}{2}\right\}}$ queries for a cascade of odd length ℓ. On the negative side, Lucks [20] presented an attack on triple encryption that, once cast into the ideal-cipher model, constitutes the best such attack known in this model by requiring roughly $2^{\kappa+n/2}$ queries.

An alternative approach to the keylength-extension problem is inspired by the key-whitening technique, first employed in the DESX construction due to Rivest. Here, the input and output of the block cipher is masked ("whitened") by an XOR with additional key material as follows: given a key tuple $(k_i, k_o, k) \in \left(\{0,1\}^{64}\right)^2 \times \{0,1\}^{56}$ a message m is mapped to

$$\mathrm{DESX}_{k_i,k_o,k}(m) = k_o \oplus \mathrm{DES}_k(k_i \oplus m).$$

The generalization of DESX for arbitrary κ, n was shown to be secure up to $2^{\frac{\kappa+n}{2}}$ queries by Kilian and Rogaway [18] even if the same key is used in both whitening steps.

In an attempt to combine cascading and key whitening, Gaži and Tessaro [17] proposed the so-called 2-XOR-cascade (or randomized cascade) construction. It consists of a cascade of length 2 interleaved with two whitening steps, mapping each n-bit message m under a key $(k, z) \in \{0,1\}^k \times \{0,1\}^n$ to

$$\mathrm{2XOR}_{k,z}(m) = E_{\widetilde{k}}(E_k(m \oplus z) \oplus z)$$

where $\widetilde{k}$ is derived from k in a deterministic way (e.g. by flipping a single bit). They prove 2-XOR-cascade to be secure up to $2^{\kappa+n/2}$ queries and also show that this bound is tight.

Other related work. There is a vast amount of literature on the security properties of different cascading-based constructions for block ciphers in various security models, in the information-theoretic setting [13,22,28,23,24,16] as well as in the computational setting [25,27,12]. The models employed in these works are however orthogonal to ours and hence the results are not directly comparable.

1.3 Our Contributions

Cascades. We start our investigation by looking at the case of a plain cascade construction of a general length ℓ (see Fig. 2). As a complement to the above-mentioned positive result given in [15], in Section 3 we present a generic attack on ℓ-cascade in our model that requires roughly $2^{\kappa+\frac{\ell-2}{\ell}n}$ queries ($2^{\kappa+\frac{\ell-1}{\ell+1}n}$ queries) for even (odd) ℓ. The well-known meet-in-the-middle attack [11] and the attack of Lucks [20] turn out to be special cases of our attack for $\ell = 2$ and $\ell = 3$, respectively. To the best of our knowledge, our result also constitutes the first formal analysis of the advantage achieved by the often-cited attack on triple encryption [20].

XOR-Cascades. After upper-bounding the security of the seemingly simplest possible construction — the cascade — we turn our attention to the more involved ℓ-XOR-cascade constructions of arbitrary length ℓ (see Fig. 4) which are a generalization of the 2-XOR-cascade proposed in [17].

In Section 4 we give a general method to reduce the security of XOR-cascades in our model to the security of so-called *key-alternating ciphers* in the random-permutation model. A key-alternating cipher (KAC) is a block cipher designed to alternate keyed XOR operations with fixed publicly known permutations (see Fig. 5). Since AES represents a prominent practical example of this design paradigm, its security has been extensively studied [10,26,19,8]. However, despite the seeming closeness to the structure of XOR-cascades, these two topics were never related to each other explicitly.

Our reduction relates the security of an XOR-cascade to the security of one step shorter KAC, allowing for more modular security analysis of XOR-cascades. By combining it with recent lower bounds on the security of KAC [10,26,19] we obtain a proof that 3-XOR-cascade and 4-XOR-cascade are secure up to $2^{\kappa+\frac{2}{3}n}$ and $2^{\kappa+\frac{3}{4}n}$ queries, respectively; and finally, that a general ℓ-XOR-cascade of odd (even) length is secure at least up to $2^{\kappa+\frac{\ell-1}{\ell+1}n}$ queries ($2^{\kappa+\frac{\ell-2}{\ell}n}$ queries), respectively.

Contrasting these results with the generic attacks on plain cascades given in Section 3, we see that a 3-XOR-cascade is provably at least as secure as a 6-cascade and a 4-XOR-cascade is at least as secure as an 8-cascade, while providing much better efficiency. This gives us a more robust argument in favor of XOR-cascades as constructions providing security and efficiency at the same time; a view that was already advocated in [17]. Note that here we are comparing security lower bounds (for XOR-cascades) to best known attacks (for plain cascades), making an even stronger case for the randomization. Alternatively, one can compare the upper bounds on distinguishing advantages for the constructions considered, we present one such comparison in Fig. 1.

Sequential Constructions. Motivated by the question of tightness of the above-mentioned bounds for XOR-cascades, we proceed by investigating generic attacks on a particular class of key-

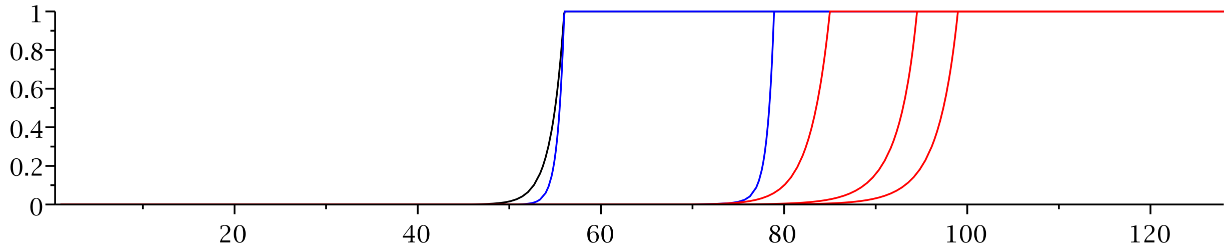

Fig. 1. Upper bounds on distinguishing advantage versus $\log_2 q$ (where q is the number of queries) for plain (blue) and randomized (red) cascades of lengths 2–4, using $\kappa = 56$ and $n = 64$. Curves from left to right: (1) single encryption for reference; (2) 2-cascade; (3) 3- and 4-cascade (same bound); (4) 2-XOR-cascade; (5) 3-XOR-cascade; (6) 4-XOR-cascade.

length extending constructions that include them. In Section 5 we look at constructions issuing ℓ queries to the block cipher while working in a sequential way: they consist of ℓ block-cipher encryptions interleaved with applications of arbitrary permutations that only depend on the key being used. For this class of constructions that we call *sequential* we exhibit an attack requiring approximately $2^{\kappa+\frac{\ell-1}{\ell}n}$ queries. Since XOR-cascades clearly belong to the class of sequential constructions, an ℓ-XOR-cascade cannot be secure beyond $2^{\kappa+\frac{\ell-1}{\ell}n}$ queries. This shows that the obtained security bounds for $\ell \in \{3, 4\}$ are tight and moreover, the ℓ-XOR-cascades of this length are optimally secure among the class of all sequential constructions, emphasizing that the extremely cheap XOR operation is sufficient to achieve the full potential of sequential constructions. This was previously only shown for $\ell = 2$ in [17].

SUMMARY. Table 1 summarizes the results of this paper in the context of previously known results. To serve as an overview, most bounds are presented in a simplified form.

Finally, note that all generic attacks presented in this paper can be mounted even if the distinguisher is only allowed to ask forward construction queries. Moreover, these queries can be chosen arbitrarily, resulting in *known-plaintext attacks*. In contrast, our security proofs are valid also with respect to an adaptive adversary allowed to ask also inverse construction queries (CCA adversary).

2 Preliminaries

2.1 Basic Notation

We typically denote sets by calligraphic letters $\mathcal{X}, \mathcal{Y}, \ldots$, and by $|\cdot|$ we denote their cardinalities. The set of all k-tuples $x^k = (x_1, \ldots, x_k)$ of elements of $\mathcal{X}$ is denoted by $\mathcal{X}^k$. The symbols $\mathrm{Func}(m, \ell)$ and $\mathrm{Perm}(n)$ refer to the sets of all functions from $\{0,1\}^m$ to $\{0,1\}^\ell$ and of all permutations of $\{0,1\}^n$, respectively; while $id \in \mathrm{Perm}(n)$ represents the identity mapping when n is implicit. All logarithms are understood to the base 2.

Random variables and concrete values they can take are usually denoted by upper-case letters $X, Y, \ldots$ and lower-case letters $x, y, \ldots$, respectively. For events A and B and random variables

ℓ	ℓ-cascade		ℓ-XOR-cascade	sequential ℓ-query construction
	security	attack	security	attack
2	$\min\{\kappa, n\}$	κ	$\kappa + \frac{n}{2}$	$\kappa + \frac{n}{2}$
3	$\kappa + \min\left\{\frac{\kappa}{2}, \frac{n}{2}\right\}$	$\kappa + \frac{n}{2}$	$\kappa + \frac{2}{3}n$ $(\star)$	$\kappa + \frac{2}{3}n$ $(\star)$
4	$\kappa + \min\left\{\frac{\kappa}{2}, \frac{n}{2}\right\}$	$\kappa + \frac{n}{2}$ $(\star)$	$\kappa + \frac{3}{4}n$ $(\star)$	$\kappa + \frac{3}{4}n$ $(\star)$
odd	$\min\left\{\frac{2\ell\kappa}{\ell+1}, \kappa + \frac{n}{2}\right\}$	$\kappa + \frac{\ell-1}{\ell+1}n$	$\kappa + \frac{\ell-1}{\ell+1}n$	$\kappa + \frac{\ell-1}{\ell}n$ $(\star)$
≥ 5		$(\star)$	$(\star)$	
even	$\min\left\{\frac{2(\ell-1)\kappa}{\ell}, \kappa + \frac{n}{2}\right\}$	$\kappa + \frac{\ell-2}{\ell}n$	$\kappa + \frac{\ell-2}{\ell}n$	

Table 1. Best known security lower bounds and generic attacks for various key-length extension schemes. Each given term is a logarithm of the respective number of queries and is parameterized by the key length κ and block size n of the underlying block cipher. References and further details to all depicted bounds are given in the text. Results denoted by $(\star)$ come from this paper.

U and V with ranges $\mathcal{U}$ and $\mathcal{V}$, respectively, we denote by $\mathsf{P}_{UA|VB}$ the corresponding conditional probability distribution, seen as a (partial) function $\mathcal{U} \times \mathcal{V} \to [0,1]$. The value $\mathsf{P}_{UA|VB}(u,v) = \mathsf{P}[U = u \wedge A | V = v \wedge B]$ is well-defined for all $u \in \mathcal{U}$ and $v \in \mathcal{V}$ such that $\mathsf{P}_{VB}(v) > 0$ and undefined otherwise. Two probability distributions P_U and $\mathsf{P}_{U'}$ on the same set $\mathcal{U}$ are equal, denoted $\mathsf{P}_U = \mathsf{P}_{U'}$, if $\mathsf{P}_U(u) = \mathsf{P}_{U'}(u)$ for all $u \in \mathcal{U}$. Conditional probability distributions are equal if the equality holds for all arguments for which both of them are defined. To emphasize the random experiment $\mathcal{E}$ in consideration, we sometimes write it in the superscript, e.g. $\mathsf{P}^{\mathcal{E}}_{U|V}(u,v)$. The expected value of a discrete random variable X is denoted by $\mathsf{E}(X) = \sum_{x \in \mathcal{X}}(x \cdot \mathsf{P}[X = x])$. The complement of an event A is denoted by $\overline{A}$.

2.2 Random Systems

To present our results we make use of Maurer's random systems framework [21], which we now introduce in a self-contained exposition sufficient to follow the rest of the paper.

We start by observing that the input-output behavior of any kind of reactive discrete system with inputs in $\mathcal{X}$ and outputs in $\mathcal{Y}$ can be described by an infinite family of functions specifying, for each $i \geq 1$, the probability distribution of the system's i-th output $Y_i \in \mathcal{Y}$ given the values of the first i inputs $X^i \in \mathcal{X}^i$ and the previous $i-1$ outputs $Y^{i-1} \in \mathcal{Y}^{i-1}$. Using this viewpoint, we say that an $(\mathcal{X}, \mathcal{Y})$-*(random) system* $\mathbf{F}$ is an infinite sequence of functions $\mathsf{p}^{\mathbf{F}}_{Y_i|X^iY^{i-1}} : \mathcal{Y} \times \mathcal{X}^i \times \mathcal{Y}^{i-1} \to [0,1]$ such that $\sum_{y_i} \mathsf{p}^{\mathbf{F}}_{Y_i|X^iY^{i-1}}(y_i, x^i, y^{i-1}) = 1$ for all $i \geq 1$, $x^i \in \mathcal{X}^i$ and $y^{i-1} \in \mathcal{Y}^{i-1}$. Note that $\mathsf{p}^{\mathbf{F}}_{Y_i|X^iY^{i-1}}$ by itself does not represent a (conditional) probability distribution in any particular random experiment with well-defined random variables Y_i, X^i, Y^{i-1} until the system is connected to a distinguisher (see below), in which case these random variables will exist and take the role of the transcript. We shall typically define discrete systems by a high level description, as long as the resulting conditional probability distributions could be derived easily from this description. A system $\mathbf{F}$ is *deterministic* if the range of $\mathsf{p}^{\mathbf{F}}_{Y_i|X^iY^{i-1}}$ is $\{0,1\}$ for all $i \geq 1$. Moreover, it is *stateless* if the probability distribution of each output depends only on the current input, i.e., if there exists a distribution $\mathsf{p}_{Y|X} : \mathcal{Y} \times \mathcal{X} \to [0,1]$ such that $\mathsf{p}^{\mathbf{F}}_{Y_i|X^iY^{i-1}}(y_i, x^i, y^{i-1}) = \mathsf{p}_{Y|X}(y_i, x_i)$ for all y_i, x^i and y^{i-1}.

A system $\mathbf{F}$ might often be used as a component (subsystem) in a construction $\mathsf{C}^{(\cdot)}$, resulting in the composed system $\mathsf{C}^{\mathbf{F}}$. While a construction $\mathsf{C}^{(\cdot)}$ does not define a random system by itself, $\mathsf{C}^{\mathbf{F}}$ does define a random system. The notions of being deterministic and of being stateless naturally extend to constructions.[1] Two (possibly dependent) systems $\mathbf{F}$ and $\mathbf{G}$ can also be composed in parallel, denoted $(\mathbf{F}, \mathbf{G})$, which simply results in a system that allows queries to both systems $\mathbf{F}$ and $\mathbf{G}$.

Examples. A special case of a random system is a *random function* $\mathbf{F} : \mathcal{X} \to \mathcal{Y}$ that implements a function f initially chosen according to some distribution on the set of all functions from $\mathcal{X}$ to $\mathcal{Y}$.[2] In particular, the *uniform random function (URF)* $\mathbf{R} : \{0,1\}^m \to \{0,1\}^\ell$ realizes a uniformly chosen function $f \in \mathrm{Func}(m, \ell)$, and the *uniform random permutation (URP)* $\mathbf{P} : \{0,1\}^n \times \{+,-\} \to \{0,1\}^n$ realizes a uniformly chosen permutation $\pi \in \mathrm{Perm}(n)$ allowing both forward queries of the form $(x,+)$ returning $\pi(x)$ as well as backward queries $(y,-)$ returning $\pi^{-1}(y)$. Throughout this paper we meet the convention that any system realizing a random function (possibly by means of a construction) which is a permutation will *always* allow both forward and backward queries. Furthermore, by $\mathbf{E} : \{0,1\}^\kappa \times \{0,1\}^n \times \{+,-\} \to \{0,1\}^n$ we denote the random function realizing an *ideal block cipher* that provides an independent uniform random permutation $\mathbf{E}_k \in \mathrm{Perm}(n)$ for each key $k \in \{0,1\}^\kappa$, allowing both forward and backward queries to each $\mathbf{E}_k$. Finally, note that with some abuse of notation, we often write $\mathbf{E}_k$ or $\mathbf{P}$ to refer to the randomly chosen permutation P implemented by the system $\mathbf{E}_k$ or $\mathbf{P}$, respectively.

Distinguishing Random Systems. A *distinguisher* $\mathbf{D}$ for an $(\mathcal{X}, \mathcal{Y})$-random system asking q queries is a $(\mathcal{Y}, \mathcal{X})$-random system which is "one query ahead:" its input-output behavior is defined by the conditional probability distributions of its queries $\mathsf{p}^{\mathbf{D}}_{X_i|X^{i-1}Y^{i-1}}$ for all $1 \leq i \leq q$. (Its first query is determined by $\mathsf{p}^{\mathbf{D}}_{X_1}$.) After the distinguisher asks all q queries, it outputs a bit W_q depending on the transcript (X^q, Y^q). Given a random system $\mathbf{F}$ and a distinguisher $\mathbf{D}$, we denote by $\mathbf{DF}$ the random experiment where $\mathbf{D}$ interacts with $\mathbf{F}$, with the distributions of the transcript (X^q, Y^q) and of the bit W_q being uniquely defined by their conditional probability distributions. For two $(\mathcal{X}, \mathcal{Y})$-random systems $\mathbf{F}$ and $\mathbf{G}$, the *distinguishing advantage* of $\mathbf{D}$ in distinguishing systems $\mathbf{F}$ and $\mathbf{G}$ by q queries is the quantity $\Delta^{\mathbf{D}}(\mathbf{F}, \mathbf{G}) = |\mathsf{P}^{\mathbf{DF}}_{W_q}(1) - \mathsf{P}^{\mathbf{DG}}_{W_q}(1)|$ and the maximal distinguishing advantage over all distinguishers asking q queries is denoted by $\Delta_q(\mathbf{F}, \mathbf{G}) = \max_{\mathbf{D}} \Delta^{\mathbf{D}}(\mathbf{F}, \mathbf{G})$ (with $\mathbf{D}$ ranging over all such distinguishers).

[1] We dispense with a formal definition. However, we point out that we allow a stateless construction to keep a state during invocations of its subsystem.

[2] As for the notion of a random variable or a random system, the word "random" does not imply any uniformity of the distribution.

If a detailed description of some distinguisher's internal workings is needed, we use standard pseudocode notation (see e.g. Fig. 3). To capture that the distinguisher issues a query x to a system $\mathbf{F}$ and stores the response as y we always use the explicit notation "**query** $y := \mathbf{F}(x)$".

Monotone Conditions. For a random system $\mathbf{F}$, we often consider an internal *monotone condition* defined on it. Such a condition is initially satisfied (true), but once it gets violated, it cannot become true again (hence the name monotone). We use such conditions to capture whether the behavior of the system meets some additional requirement (e.g. distinct outputs, consistent outputs) or this was already violated during the interaction that occurred so far. A monotone condition is formalized by a sequence of events $\mathcal{A} = A_0, A_1, \ldots$ such that A_0 always holds, and A_i holds if the condition holds after answering the i-th query. The probability that a distinguisher $\mathbf{D}$ issuing q queries to $\mathbf{F}$ makes a monotone condition $\mathcal{A}$ fail in the random experiment $\mathbf{DF}$ is denoted by $\nu^{\mathbf{D}}(\mathbf{F}, \overline{A_q}) = \mathsf{P}^{\mathbf{DF}}(\overline{A_q})$ and maximum over all such distinguishers is denoted by $\nu(\mathbf{F}, \overline{A_q}) = \max_{\mathbf{D}} \nu^{\mathbf{D}}(\mathbf{F}, \overline{A_q})$.

For any random system $\mathbf{F}$ with a monotone condition $\mathcal{A}$ defined on it, following [24] we define $\mathbf{F}$ *blocked by* $\mathcal{A}$ to be a new random system that behaves exactly like $\mathbf{F}$ as long as the condition $\mathcal{A}$ is satisfied; but once $\mathcal{A}$ is violated, it only outputs a special blocking symbol $\perp$ not contained in the output alphabet of $\mathbf{F}$. We will make use of the following helpful claims on random systems proven in previous works.

Lemma 1. *Let $\mathsf{C}^{(\cdot)}$ and $\mathsf{C}'^{(\cdot)}$ be two constructions invoking a subsystem, and let $\mathbf{F}$ and $\mathbf{G}$ be random systems. Let $\mathcal{A}$ and $\mathcal{B}$ be two monotone conditions defined on $\mathbf{F}$ and $\mathbf{G}$, respectively.*

(i) [15, Lemma 2] Let $\mathbf{F}^{\perp}$ denote the random system $\mathbf{F}$ blocked by $\mathcal{A}$ and let $\mathbf{G}^{\perp}$ denote $\mathbf{G}$ blocked by $\mathcal{B}$. Then for every distinguisher $\mathbf{D}$ asking q queries we have $\Delta^{\mathbf{D}}(\mathbf{F}, \mathbf{G}) \leq \Delta_q(\mathbf{F}^{\perp}, \mathbf{G}^{\perp}) + \nu^{\mathbf{D}}(\mathbf{F}, \overline{A_q})$.

(ii) [21, Lemma 5] $\Delta_q(\mathsf{C}^{\mathbf{F}}, \mathsf{C}^{\mathbf{G}}) \leq \Delta_{q'}(\mathbf{F}, \mathbf{G})$, where q' is the maximum number of invocations of any internal system $\mathbf{H}$ for any sequence of q queries to $\mathsf{C}^{\mathbf{H}}$, if such a value is defined.

(iii) [15, Lemma 3] There exists a fixed permutation $S \in \mathrm{Perm}(n)$ (represented by a deterministic stateless system) such that $\Delta_q(\mathsf{C}^{\mathbf{P}}, \mathsf{C}'^{\mathbf{P}}) \leq \Delta_q(\mathsf{C}^{S}, \mathsf{C}'^{S})$.

3 Plain Cascades

We start by investigating the security of the plain cascade construction. Having a lower bound on the security of plain cascades given in [15], it is natural to approach the question from the opposite direction and explore generic attacks on the cascade construction in our model. In this section we describe such an attack for the general case of a cascade of arbitrary length $\ell \geq 2$. It shows that, roughly speaking, plain cascade of length ℓ can be attacked in $2^{\kappa + \frac{\ell-2}{\ell}n}$ queries ($2^{\kappa + \frac{\ell-1}{\ell+1}n}$ queries) for even (odd) ℓ.

Let $\mathsf{Casc}_{\ell}^{(\cdot)} \colon (\{0,1\}^{\kappa})^{\ell} \times \{0,1\}^n \times \{+,-\} \to \{0,1\}^n$ denote a (deterministic stateless) construction which expects a subsystem $\mathbf{E} \colon \{0,1\}^{\kappa} \times \{0,1\}^n \times \{+,-\} \to \{0,1\}^n$ realizing a block cipher. $\mathsf{Casc}_{\ell}^{\mathbf{E}}$ then realizes cascaded encryption of length ℓ using the block cipher $\mathbf{E}$ and the keys given,

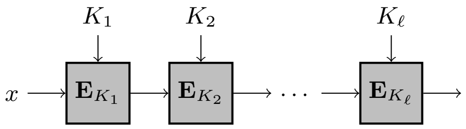

Fig. 2. The cascade construction realized by $\mathsf{Casc}^{\mathbf{E}}_{\ell,\bar{K}}$.

i.e., $\mathsf{Casc}^{\mathbf{E}}_{\ell}$ answers each forward query $(k_1, \ldots, k_\ell, x, +)$ by $\mathbf{E}_{k_\ell}(\cdots \mathbf{E}_{k_1}(x) \cdots)$ and each backward query $(k_1, \ldots, k_\ell, y, -)$ by $\mathbf{E}^{-1}_{k_1}(\cdots \mathbf{E}^{-1}_{k_\ell}(y) \cdots)$. Moreover, we let $\mathsf{Casc}^{\mathbf{E}}_{\ell,\bar{K}}$ be the system that chooses a uniformly random (secret) key tuple $\bar{K} = (K_1, \ldots, K_\ell) \in (\{0,1\}^\kappa)^\ell$ and then gives access to the permutation $\mathsf{Casc}^{\mathbf{E}}_{\ell}(\bar{K}, \cdot)$ in both directions (i.e., takes inputs from $\{0,1\}^n \times \{+,-\}$). The evaluation of a forward query by $\mathsf{Casc}^{\mathbf{E}}_{\ell,\bar{K}}$ is depicted in Fig. 2.

Theorem 1. *For the cascade construction* $\mathsf{Casc}^{(\cdot)}_{\ell,\bar{K}}$ *of even length* $\ell \geq 2$ *using an ideal block cipher* $\mathbf{E}$ *and for any*[3] *parameter* $0 < t < 2^{2n/\ell - 1}$ *there exists a distinguisher* $\mathbf{D}$ *such that*

$$\Delta^{\mathbf{D}}\left((\mathbf{E}, \mathsf{Casc}^{\mathbf{E}}_{\ell,\bar{K}}), (\mathbf{E}, \mathbf{P})\right) \geq 1 - \frac{2}{t} - 2^{\ell\kappa - t(n-1)}$$

and $\mathbf{D}$ *asks at most* $\ell \cdot 2^{\kappa + \frac{\ell-2}{\ell}n}$ *queries to* $\mathbf{E}$ *and* $2t \cdot 2^{\frac{\ell-2}{\ell}n}$ *forward queries to either of* $\mathsf{Casc}^{\mathbf{E}}_{\ell,\bar{K}}$ *and* $\mathbf{P}$. *For odd-length cascades,* $\mathbf{D}$ *requires at most* $\ell \cdot 2^{\kappa + \frac{\ell-1}{\ell+1}n}$ *queries to* $\mathbf{E}$ *and* $2t \cdot 2^{\frac{\ell-1}{\ell+1}n}$ *forward queries to either of* $\mathsf{Casc}^{\mathbf{E}}_{\ell,\bar{K}}$ *and* $\mathbf{P}$.

Proof. Assume ℓ is even, we give the description of the distinguisher $\mathbf{D}$ in Fig. 3. It first chooses an arbitrary set $\mathcal{S}_0 \subseteq \{0,1\}^n$ and independent random sets $\mathcal{S}_2, \mathcal{S}_4, \ldots, \mathcal{S}_{\ell-2} \subseteq \{0,1\}^n$ of the given sizes and issues $2t \cdot 2^{\frac{\ell-2}{\ell}n}$ queries to the construction (cascade or random permutation – let us denote it $\mathbf{S}$) to obtain $\mathcal{S}_\ell := \mathbf{S}(\mathcal{S}_0)$. Each $\mathcal{S}_i$ will represent the subset of values $\{0,1\}^n$ that $\mathbf{D}$ "cares about" after i steps of the cascade. Then $\mathbf{D}$ issues $\ell \cdot 2^{\kappa + \frac{\ell-2}{\ell}n}$ block-cipher queries to obtain all the values

$$\mathbf{E}_k(\mathcal{S}_0), \mathbf{E}^{-1}_k(\mathcal{S}_2), \mathbf{E}_k(\mathcal{S}_2), \ldots, \mathbf{E}^{-1}_k(\mathcal{S}_{\ell-2}), \mathbf{E}_k(\mathcal{S}_{\ell-2}), \mathbf{E}^{-1}_k(\mathcal{S}_\ell)$$

with all possible keys $k \in \{0,1\}^\kappa$. These are all the queries $\mathbf{D}$ makes, it remains to justify that they are sufficient to expect that there is a constant number of values $x \in \{0,1\}^n$ that, in case the correct keys are guessed, can be traced through the whole cascade only with the information obtained above. Each such path then allows us to compare its endpoint with $\mathbf{S}(x)$ which will most probably only match if $\mathbf{S}$ is the cascade.

Let us analyze the probability that the set $\mathcal{I}$ is found on line 14 in the setting where $\mathbf{S} = \mathsf{Casc}^{\mathbf{E}}_{\ell.\bar{K}}$ and the examined key is the correct one, i.e., for $\bar{k}$ chosen on line 13 we have $\bar{k} = \bar{K}$. Consider the

[3] For some intuition about the bound obtained, consider e.g. $\kappa \approx n$ and $t :\approx \ell + 1$.

```
Distinguisher $\mathbf{D}(\mathbf{E},\mathbf{S})$:                 where $\mathbf{S} \in \{\mathsf{Casc}^{\mathbf{E}}_{\ell.\bar{K}}, \mathbf{P}\}$
 1: choose arbitrary $\mathcal{S}_0 \subseteq \{0,1\}^n$ s.t. $|\mathcal{S}_0| = 2t \cdot 2^{\frac{\ell-2}{\ell}n}$
 2: for $i := 1$ to $\ell/2 - 1$ do
 3:     choose uniformly at random $\mathcal{S}_{2i} \subseteq \{0,1\}^n$ s.t. $|\mathcal{S}_{2i}| = 2^{\frac{\ell-2}{\ell}n}$
 4: for all $x \in \mathcal{S}_0$ do
 5:     query $y(x) := \mathbf{S}(x,+)$
 6: $\mathcal{S}_\ell := \{y(x) \mid x \in \mathcal{S}_0\}$
 7: for all $x \in \mathcal{S}_0 \cup \mathcal{S}_2 \cup \cdots \cup \mathcal{S}_{\ell-2}$ do
 8:     for all $k \in \{0,1\}^\kappa$ do
 9:         query $e_k(x) := \mathbf{E}(k,x,+)$
10: for all $y \in \mathcal{S}_2 \cup \mathcal{S}_4 \cup \cdots \cup \mathcal{S}_\ell$ do
11:     for all $k \in \{0,1\}^\kappa$ do
12:         query $e_k^{-1}(y) := \mathbf{E}(k,y,-)$
13: for all $\bar{k} = (k_1,\ldots,k_\ell) \in (\{0,1\}^\kappa)^\ell$ do
14:     choose $\mathcal{I} \subseteq \mathcal{S}_0$ s.t. $|\mathcal{I}| = t$ and $\forall x \in \mathcal{I}, \forall i \in \{1,\ldots,\ell\}$ :
          $e_{k_i}(\cdots e_{k_1}(x))$ is known from lines 9 and 12
15:     if $\mathcal{I}$ exists $\wedge\ \forall x \in \mathcal{I} : y(x) = e_{k_\ell}(\cdots e_{k_1}(x))$ then
16:         return 1
17: return 0
```

Fig. 3. Distinguisher $\mathbf{D}$ for the proof of Theorem 1 for the case of ℓ being even.

sets

$$\begin{aligned} \mathcal{P}_0 &= \mathcal{S}_0 \\ \mathcal{P}_2 &= \mathbf{E}^{-1}_{k_1}(\mathbf{E}^{-1}_{k_2}(\mathcal{S}_2)) \\ &\vdots \\ \mathcal{P}_{\ell-2} &= \mathbf{E}^{-1}_{k_1}(\cdots \mathbf{E}^{-1}_{k_{\ell-3}}(\mathbf{E}^{-1}_{k_{\ell-2}}(\mathcal{S}_{\ell-2}))\cdots), \end{aligned}$$

i.e., $\mathcal{P}_{2i}$ for $i \geq 1$ is the subset of the plaintext space $\{0,1\}^n$ that gets mapped to $\mathcal{S}_{2i}$ after applying the first $2i$ steps of the cascade with the correct keys. Since the sets $\mathcal{S}_{2i}$ for $i \geq 1$ were chosen independently at random, we can invoke Lemma 2 (given in Appendix A) to obtain that for $\mathcal{P} = \bigcap_{i=0}^{\ell/2-1} \mathcal{P}_{2i}$ we have

$$\mathsf{E}(|\mathcal{P}|) = \frac{\prod_{i=0}^{\ell/2-1} |\mathcal{P}_{2i}|}{2^{n\left(\frac{\ell}{2}-1\right)}} = \frac{\prod_{i=0}^{\ell/2-1} |\mathcal{S}_{2i}|}{2^{n\left(\frac{\ell}{2}-1\right)}} = 2t$$

and similarly $\mathsf{Var}(|\mathcal{P}|) \leq 2t$. Using Chebyshev inequality, this gives us $\mathsf{P}(|\mathcal{P}| < t) \leq 2/t$. If this does not occur (i.e., if $|\mathcal{P}| \geq t$) then any t-element subset of $\mathcal{P}$ clearly satisfies all requirements imposed on the set $\mathcal{I}$ on lines 14 and 15 (note that any such subset can be chosen, we assume that $\mathbf{D}$ has a fixed way of doing so). Since the desired $\mathcal{I}$ exists, $\mathbf{D}$ will output 1 in this case. Overall, this gives us that $\mathbf{D}(\mathbf{E}, \mathsf{Casc}^{\mathbf{E}}_{\ell.\bar{K}})$ outputs 1 with probability at least $1 - 2/t$.

On the other hand, if $\mathbf{S} = \mathbf{P}$ then for each $\bar{k}$ the condition on line 15 can only be satisfied with probability at most $2^{-t(n-1)}$, hence by union bound $\mathbf{D}(\mathbf{E},\mathbf{P})$ outputs 1 with probability at most $2^{\ell\kappa - t(n-1)}$, which concludes the proof for the case of even ℓ.

For odd ℓ we just start by choosing $\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_3, \ldots, \mathcal{S}_{\ell-2} \subseteq \{0,1\}^n$ with $|\mathcal{S}_0| = 2t \cdot 2^{\frac{\ell-1}{\ell+1}n}$ and each of the remaining sets having size $2^{\frac{\ell-1}{\ell+1}n}$. The rest of the attack and its analysis is analogous and therefore omitted. □

Interestingly, for $\ell = 2$ our attack corresponds to the well-known meet-in-the-middle attack against double encryption [11] and for $\ell = 3$ it corresponds to one of the attacks given in [20].

Note that there is a trade-off between the number of construction queries and block cipher queries required for the attack presented in Theorem 1. The attack can be generalized to require a lower number $2tm$ of construction queries and $2^{\kappa+n-\frac{2\log m}{\ell-2}}$ block cipher queries. Moreover, the construction queries can be chosen arbitrarily, making it a known-plaintext attack.

4 XOR-Cascades

We now turn to investigate the so-called XOR-cascades that, loosely speaking, consist of several encryption steps interleaved with key-whitening steps using the XOR operation.

This design paradigm still offers several degrees of freedom: the addition or omission of the key-whitening step at the beginning and at the end; as well as repetition or dependence of keys across the encryption and whitening steps. We resolve the first choice by including the first XOR operation and omitting the last one, see Fig. 4 and the formal definition below. In the choice of key-scheduling we consider the variant that derives all keys used in the encryption steps from a single one in a fixed deterministic way such that they are distinct. This is safe thanks to the properties of the ideal-cipher model that we are working in that postulates the independence of the permutations realized for each key by the block cipher. In order to weaken this assumption, one could also consider independent keys for each of the encryption steps. Finally, we assume the whitening keys to be random and independent. A formal definition of the ℓ-XOR-cascade construction follows.

Let us fix a deterministic way to derive ℓ distinct κ-bit keys $(k^{(1)}, \ldots, k^{(\ell)})$ from a given κ-bit key k in such a way that each mapping $k \mapsto k^{(i)}$ is a bijection. For example, if we assume $\ell \leq \kappa$ then we can simply set $k^{(i)} := k \oplus 0^{i-1}10^{\kappa-i}$, i.e., $k^{(i)}$ will differ from k in the i-th bit. The definition extends naturally to random variables $K^{(1)}, \ldots, K^{(\ell)}$ derived from a uniformly random key K.

In the following discussion, let us model the XOR-Cascade of length ℓ by a (deterministic stateless) construction $\mathsf{X}_\ell^{(\cdot)} \colon \{0,1\}^\kappa \times (\{0,1\}^n)^{\ell+1} \times \{+,-\} \to \{0,1\}^n$ which expects to access a subsystem $\mathbf{E} \colon \{0,1\}^\kappa \times \{0,1\}^n \times \{+,-\} \to \{0,1\}^n$ realizing a block cipher. The combined system $\mathsf{X}_\ell^{\mathbf{E}}$ then answers each forward query $(k, z_1, \ldots, z_\ell, x, +)$ by $\mathbf{E}_{k^{(\ell)}}(\cdots \mathbf{E}_{k^{(2)}}(\mathbf{E}_{k^{(1)}}(x \oplus z_1) \oplus z_2) \cdots \oplus z_\ell)$ and each backward query $(k, z_1, \ldots, z_\ell, y, -)$ by $\mathbf{E}^{-1}_{k^{(1)}}(\cdots \mathbf{E}^{-1}_{k^{(\ell-1)}}(\mathbf{E}^{-1}_{k^{(\ell)}}(y) \oplus z_\ell) \oplus z_{\ell-1} \cdots) \oplus z_1$. Again, we let $\mathsf{X}^{\mathbf{E}}_{\ell,K,\bar{Z}}$ be the system that first chooses uniformly random (secret) keys $(K, \bar{Z}) \in \{0,1\}^\kappa \times (\{0,1\}^n)^\ell$ where $\bar{Z} = (Z_1, \ldots, Z_\ell)$ and then gives access to the permutation $\mathsf{X}_\ell^{\mathbf{E}}(K, \bar{Z}, \cdot)$ in both directions (i.e., takes inputs from $\{0,1\}^n \times \{+,-\}$). The evaluation of a forward query by $\mathsf{X}^{\mathbf{E}}_{\ell,K,\bar{Z}}$ is depicted in Fig. 4.

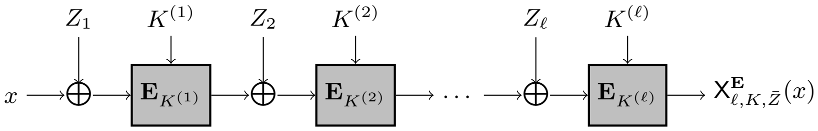

Fig. 4. The XOR-cascade construction realized by $\mathsf{X}^{\mathbf{E}}_{\ell,K,\bar{Z}}$.

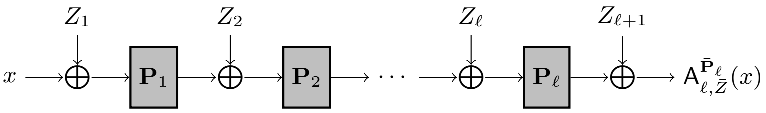

Fig. 5. The key-alternating cipher realized by $\mathsf{A}^{\bar{\mathbf{P}}_\ell}_{\ell,\bar{Z}}$.

Before presenting our results, we introduce the notion of *key-alternating ciphers.* This concept, studied for example in [14,10,26,19,8], is surprisingly close to the notion of XOR-cascades, however introduced with a very different motivation. It refers to a construction of a block cipher by alternating two types of steps: an XOR of a secret key and an application of a publicly known permutation (see Fig. 5 and the formal definition below). A prominent example of a block cipher having this structure is the current standard AES [4]. This approach to block-cipher construction is then typically studied in the random-permutation model where one assumes that the permutation steps consist of applications of uniformly random and independent, publicly accessible permutations. Below we model the key-alternating ciphers under this assumption. Note that in this setting it is natural to consider constructions that both start and end with the XOR operation.

Let us denote by $\mathsf{A}^{(\cdot)}_{\ell,\bar{Z}}$ the key-alternating cipher as it is formalized in the random permutation model (e.g. in [14,10,26,19]). More precisely, let $\mathsf{A}^{(\cdot)}_{\ell}\colon\ (\{0,1\}^n)^{\ell+2} \times \{+,-\} \to \{0,1\}^n$ be a construction which expects to access a subsystem $\hat{\mathbf{P}}_\ell$ giving bidirectional access to ℓ arbitrary permutations (denoted $P_1,\ldots,P_\ell$), using some fixed addressing mechanism for the queries. The combined system $\mathsf{A}^{\hat{\mathbf{P}}_\ell}_{\ell}$ then answers each forward query $(z_1,\ldots,z_{\ell+1},x,+)$ by $P_\ell\left(\cdots P_2\left(P_1\left(x \oplus z_1\right) \oplus z_2\right) \cdots \oplus z_\ell\right) \oplus z_{\ell+1}$ and each backward query $(z_1,\ldots,z_{\ell+1},y,-)$ by $P_1^{-1}(\cdots P_{\ell-1}^{-1}(P_\ell^{-1}(y \oplus z_{\ell+1}) \oplus z_\ell) \oplus z_{\ell-1} \cdots) \oplus z_1$. Again, we let $\mathsf{A}^{\hat{\mathbf{P}}_\ell}_{\ell,\bar{Z}}$ be the system that first chooses uniformly random (secret) keys $\bar{Z} \in (\{0,1\}^n)^{\ell+1}$ where $\bar{Z} = (Z_1,\ldots,Z_{\ell+1})$ and then gives access to the permutation $\mathsf{A}^{\hat{\mathbf{P}}_\ell}_{\ell}(\bar{Z},\cdot)$ in both directions (taking inputs from $\{0,1\}^n \times \{+,-\}$). Finally, let $\bar{\mathbf{P}}_i$ denote a system that provides bidirectional access to i independent uniformly random permutations. The evaluation of a forward query by $\mathsf{A}^{\bar{\mathbf{P}}_\ell}_{\ell,\bar{Z}}$ is depicted in Fig. 5 and some known results on the security of key-alternating ciphers in the random-permutation model are summarized using our formalism in Appendix B.

We are now ready to present the reduction of the security of XOR-cascades in the ideal-cipher model to the problem of the security of one step shorter key-alternating ciphers in the random-permutation model. This reduction allows one to analyze the problem in a simpler setting without considering the block-cipher keys, as well as invoke existing results on key-alternating ciphers. The proof modularizes the approach used in [17] to analyze the security of XOR-cascade of length 2 and generalizes it to arbitrary lengths.

Theorem 2. *For $\ell \geq 2$, for the constructions $\mathsf{X}^{(\cdot)}_{\ell,K,\bar{Z}}$ and $\mathsf{A}^{(\cdot)}_{\ell-1,\bar{Z}}$ defined as above, and for every distinguisher $\mathbf{D}$ making q queries to $\mathbf{E}$,*

$$\Delta^{\mathbf{D}}\left(\left(\mathbf{E},\mathsf{X}^{\mathbf{E}}_{\ell,K,\bar{Z}}\right),(\mathbf{E},\mathbf{P})\right) \leq \min_{h}\left\{\frac{\ell q}{h2^{\kappa}} + \Delta_h\left(\left(\bar{\mathbf{P}}_{\ell-1},\mathsf{A}^{\bar{\mathbf{P}}_{\ell-1}}_{\ell-1,\bar{Z}}\right),\bar{\mathbf{P}}_{\ell}\right)\right\}.$$

In particular, $\mathbf{D}$ can make arbitrarily many queries to either of $\mathsf{X}^{\mathbf{E}}_{\ell,K,\bar{Z}}$ and $\mathbf{P}$.

Proof. In accordance with [9,15,17] we first reduce the original distinguishing problem to a simpler one, involving only block-cipher queries. Overall, the system $(\mathbf{E},\mathsf{X}^{\mathbf{E}}_{\ell,K,\bar{Z}})$ provides an interface to query $2^{\kappa}+1$ (dependent) permutations: 2^{κ} of them correspond to the block cipher $\mathbf{E}$ being used under all possible keys and the last permutation is provided by $\mathsf{X}^{\mathbf{E}}_{\ell,K,\bar{Z}}$, where the values K and $\bar{Z}$ are chosen at the beginning by the construction $\mathsf{X}_{\ell,K,\bar{Z}}$. (All these permutations can be queried both in forward and backward direction.) Since the last permutation is also uniformly distributed and Perm(n) forms a group under composition, the joint distribution of these permutations does not change if we first choose the last permutation uniformly at random, i.e., we replace it by $\mathbf{P}$, then pick random K and $\bar{Z}$ and finally choose the permutations of the block cipher independently and uniformly for all keys except $K^{(\ell)}$, for which we choose the permutation $x \mapsto \mathbf{P}(\mathbf{E}^{-1}_{K^{(1)}}(\cdots\mathbf{E}^{-1}_{K^{(\ell-2)}}(\mathbf{E}^{-1}_{K^{(\ell-1)}}(x\oplus Z_{\ell})\oplus Z_{\ell-1})\cdots)\oplus Z_1)$. To formalize this transition, let $\mathsf{G}^{(\cdot)}$ be a construction that expects a single permutation as its subsystem (let us denote it P) and itself provides an interface to a block cipher (let us denote it G). Any query to G is answered in the following way: in advance, G chooses random keys $(K,\bar{Z})$ and then generates random independent permutations for G used with any key except $K^{(\ell)}$. For $K^{(\ell)}$, G instead realizes the permutation $x \mapsto P(G^{-1}_{K^{(1)}}(\cdots G^{-1}_{K^{(\ell-2)}}(G^{-1}_{K^{(\ell-1)}}(x\oplus Z_{\ell})\oplus Z_{\ell-1})\cdots)\oplus Z_1)$, querying P for any necessary values. By the above argument we then have $\left(\mathbf{E},\mathsf{X}^{\mathbf{E}}_{\ell,K,\bar{Z}}\right)=(\mathsf{G}^{\mathbf{P}},\mathbf{P})$ and hence also

$$\Delta_q\left(\left(\mathbf{E},\mathsf{X}^{\mathbf{E}}_{\ell,K,\bar{Z}}\right),(\mathbf{E},\mathbf{P})\right)=\Delta_q\left(\left(\mathsf{G}^{\mathbf{P}},\mathbf{P}\right),(\mathbf{E},\mathbf{P})\right).$$

Now we can apply claim (iii) in Lemma 1 to obtain $\Delta_q\left(\left(\mathsf{G}^{\mathbf{P}},\mathbf{P}\right),(\mathbf{E},\mathbf{P})\right) \leq \Delta_q\left(\left(\mathsf{G}^{S},S\right),(\mathbf{E},S)\right)$ where S denotes the fixed permutation whose existence is guaranteed by this claim. Since S is fixed and hence can be seen as known to the distinguisher, it makes no sense to query it and therefore we only have to bound $\Delta_q\left(\mathsf{G}^{S},\mathbf{E}\right)$ for an arbitrary permutation S. To simplify the notation, we shall denote the system G^{S} by $\mathbf{G}$.

Let us call a (forward or backward) query to $\mathbf{G}$ *relevant* if it involves any of the keys $K^{(1)},\ldots,K^{(\ell)}$. Similarly, we can see the system $\mathbf{E}$ as also choosing some random key K (and hence also all $K^{(i)}$)

that does not affect its behavior, it just serves to define relevant queries for $\mathbf{E}$ in an analogous way. We now define monotone conditions $\mathcal{A}^h$ and $\mathcal{B}^h$ on systems $\mathbf{E}$ and $\mathbf{G}$ respectively, such that each of these conditions remains satisfied as long as at most h of the queries asked so far were relevant. In $\mathbf{E}$ the probability of violating this condition can be upper-bounded easily since the keys $K^{(i)}$ do not affect the system's behavior and hence it suffices to consider non-adaptive strategies. The expected number of relevant queries among any given q queries asked by the distinguisher is $\ell q \cdot 2^{-\kappa}$ and from Markov inequality we obtain $\nu(\mathbf{E}, \overline{\mathcal{A}}_q^h) \leq \ell q / h 2^\kappa$. Hence by claim (i) of Lemma 1 we have

$$\Delta_q(\mathbf{G}, \mathbf{E}) \leq \Delta_q(\mathbf{G}^\perp, \mathbf{E}^\perp) + \nu(\mathbf{E}, \overline{\mathcal{A}}_q^h) \leq \Delta_q(\mathbf{G}^\perp, \mathbf{E}^\perp) + \ell q / h 2^\kappa$$

where $\mathbf{E}^\perp$ and $\mathbf{G}^\perp$ denote the systems $\mathbf{E}$ and $\mathbf{G}$ blocked by $\mathcal{A}^h$ and $\mathcal{B}^h$, respectively.

In order to upper-bound the term $\Delta_q(\mathbf{G}^\perp, \mathbf{E}^\perp)$, we notice that the systems $\mathbf{G}^\perp$ and $\mathbf{E}^\perp$ only differ in a small part. Moreover, this part corresponds to the systems considered in the security definition of key-alternating ciphers in the random-permutation model. More precisely, $\mathbf{G}^\perp = \mathsf{C}^{\mathbf{S}}$ and $\mathbf{E}^\perp = \mathsf{C}^{\mathbf{T}}$ where:

- $\mathbf{S}$ denotes a system that chooses ℓ random keys $\bar{Z} \in (\{0,1\}^n)^\ell$ and then provides access (by means of both forward and backward queries) to ℓ randomly chosen permutations $\pi_1, \ldots, \pi_\ell \in \mathrm{Perm}(n)$ such that they satisfy the equation

  $$\pi_\ell^{-1}(\pi_{\ell-1}(\cdots \pi_2(\pi_1(\cdot \oplus Z_1) \oplus Z_2) \oplus Z_3 \cdots) \oplus Z_\ell) = id;$$

  i.e., $\pi_1, \ldots, \pi_{\ell-1}$ are chosen independently at random and π_ℓ is set to

  $$x \mapsto \pi_{\ell-1}(\cdots \pi_2(\pi_1(x \oplus Z_1) \oplus Z_2) \oplus Z_3 \cdots) \oplus Z_\ell.$$

  Note that this corresponds to the system $\left(\bar{\mathbf{P}}_{\ell-1}, \mathsf{A}_{\ell-1,\bar{Z}}^{\bar{\mathbf{P}}_{\ell-1}}\right)$.
- $\mathbf{T}$ denotes a system that provides access (by means of both forward and backward queries) to ℓ uniformly random permutations $\pi_1, \ldots, \pi_\ell \in \mathrm{Perm}(n)$ that are independent. This in turn corresponds to the system $\bar{\mathbf{P}}_\ell$.
- $\mathsf{C}^{(\cdot)}$ denotes a randomized construction expecting a subsystem providing bidirectional access to ℓ permutations $\pi_1, \ldots, \pi_\ell$. The construction $\mathsf{C}^{(\cdot)}$ itself then provides access to a block cipher (let us denote it C) as follows: it first chooses a uniformly random key K and then sets $C_{K^{(i)}} := \pi_i$ for all $i \in \{1, \ldots, \ell - 1\}$ and $C_{K^{(\ell)}}(\cdot) := S(\pi_\ell^{-1}(\cdot))$. ($\mathsf{C}$ only queries its subsystem once it is necessary in order to answer a relevant query to C). The permutations for all other keys are chosen independently at random and maintained by C. Moreover, C only allows h relevant queries, after that it returns $\perp$.

It is now straightforward to verify that we indeed have $\mathbf{G}^\perp = \mathsf{C}^{\mathbf{S}}$ and $\mathbf{E}^\perp = \mathsf{C}^{\mathbf{T}}$. Since $\mathsf{C}^{(\cdot)}$ issues at most h queries to its subsystem, we can invoke Lemma 1(ii) to obtain

$$\Delta_q(\mathbf{G}^\perp, \mathbf{E}^\perp) \leq \Delta_h(\mathbf{S}, \mathbf{T}) = \Delta_h\left(\left(\bar{\mathbf{P}}_{\ell-1}, \mathsf{A}_{\ell-1,\bar{Z}}^{\bar{\mathbf{P}}_{\ell-1}}\right), \bar{\mathbf{P}}_\ell\right).$$

The whole argument holds for any parameter h, hence we can minimize over it to conclude the proof of the theorem. □

Combining our Theorem 2 with the known results on the security of key-alternating ciphers in the random permutation model [10,26,19] given in Appendix B we obtain the following corollary.

Corollary 1. *Let $\mathsf{X}^{(\cdot)}_{\ell,K,\bar{Z}}$ denote the ℓ-XOR-cascade construction as above. Then we have:*

1. *3-XOR-cascade is secure up to roughly $2^{\kappa+\frac{2}{3}n}$ queries; more precisely, for $n \geq 20$ we have*
$$\varDelta_q\left(\left(\mathbf{E},\mathsf{X}^{\mathbf{E}}_{3,K,\bar{Z}}\right),(\mathbf{E},\mathbf{P})\right) \leq 3\cdot\left(\frac{q}{2^{\kappa+\frac{2}{3}n}}\right)^{\frac{1}{2}} + 9\cdot\left(\frac{q}{2^{\kappa+\frac{2}{3}n}}\right)^{\frac{3}{2}} + 3\cdot\frac{q}{2^{\kappa+\frac{2}{3}n}}\ .$$
2. *ℓ-XOR-cascade is secure up to roughly $2^{\kappa+\frac{3}{4}n}$ queries for $\ell \geq 4$; more precisely, for $n \geq 27$ we have*
$$\varDelta_q\left(\left(\mathbf{E},\mathsf{X}^{\mathbf{E}}_{\ell,K,\bar{Z}}\right),(\mathbf{E},\mathbf{P})\right) \leq \ell\cdot\left(\frac{q}{2^{\kappa+\frac{3}{4}n}}\right)^{\frac{1}{2}} + 9\cdot\frac{q}{2^{\kappa+\frac{3}{4}n}} + 4\cdot\left(\frac{q}{2^{\kappa+\frac{3}{4}n}}\right)^{\frac{3}{2}}\ .$$
3. *ℓ-XOR-cascade is secure up to roughly $2^{\kappa+\frac{\ell-1}{\ell+1}n}$ queries for odd ℓ; more precisely, we have*
$$\varDelta_q\left(\left(\mathbf{E},\mathsf{X}^{\mathbf{E}}_{\ell,K,\bar{Z}}\right),(\mathbf{E},\mathbf{P})\right) \leq (\ell+1)\cdot\left(\frac{q}{2^{\kappa+\frac{\ell-1}{\ell+1}n}}\right)^{\frac{1}{2}} + 2^{3+\frac{\ell-1}{4}}\cdot\left(\frac{q}{2^{\kappa+\frac{\ell-1}{\ell+1}n}}\right)^{\frac{\ell+1}{8}}\ .$$

For even ℓ one can prove the same security as for one step shorter odd-length XOR-cascade.

Proof (sketch). We combine the statement of Theorem 2 with the bounds on the security of the key-alternating cipher listed in Theorem 4, choosing the value h to be $q^{\frac{1}{2}}2^{\frac{n}{3}-\frac{\kappa}{2}}$, $q^{\frac{1}{2}}2^{\frac{3n}{8}-\frac{\kappa}{2}}$ and $q^{\frac{1}{2}}2^{\frac{(\ell-1)n}{2(\ell+1)}-\frac{\kappa}{2}}$ in the three cases above, respectively. The statements for constructions with more rounds follow from the fact that
$$\varDelta_h\left(\left(\bar{\mathbf{P}}_\ell,\mathsf{A}^{\bar{\mathbf{P}}_\ell}_{\ell,\bar{Z}}\right),\bar{\mathbf{P}}_{\ell+1}\right) \leq \varDelta_h\left(\left(\bar{\mathbf{P}}_{\ell-1},\mathsf{A}^{\bar{\mathbf{P}}_{\ell-1}}_{\ell-1,\bar{Z}}\right),\bar{\mathbf{P}}_\ell\right)$$
which can be shown by a straightforward reduction. □

Note that our result implies that with increasing length ℓ, XOR-cascade approaches the security level $2^{\kappa+n}$ which is optimal in our model.

5 Sequential Constructions

To obtain an upper bound on the security achievable by the ℓ-XOR-cascade construction, in this section we consider keylength-extending constructions having a particular natural form which we call *sequential.*

A construction $\mathsf{C}\colon \{0,1\}^{\kappa'} \times \{0,1\}^n \times \{+,-\} \to \{0,1\}^n$ is sequential if, given an underlying block cipher $\mathbf{E}$, the mapping it realizes can be written as
$$\mathsf{C}^{\mathbf{E}}(k',x,+) = Q_{\ell,k'}\left(\mathbf{E}_{k_\ell}\left(Q_{\ell-1,k'}\left(\cdots\mathbf{E}_{k_2}\left(Q_{1,k'}\left(\mathbf{E}_{k_1}\left(Q_{0,k'}(x)\right)\right)\right)\cdots\right)\right)\right)$$

```
Distinguisher $\mathbf{D}(\mathbf{E}, \mathbf{S})$:                where $\mathbf{S} \in \{\mathsf{C}^{\mathbf{E}}_{K'}, \mathbf{P}\}$
 1: for all $x \in \{0,1\}^n$ do
 2:     query $y(x) := \mathbf{S}(x, +)$
 3: choose uniformly at random $\mathcal{S}_1 \subseteq \{0,1\}^n$ s.t. $|\mathcal{S}_1| = 2t \cdot 2^{\frac{\ell-1}{\ell}n}$
 4: for $i := 2$ to $\ell$ do
 5:     choose uniformly at random $\mathcal{S}_i \subseteq \{0,1\}^n$ s.t. $|\mathcal{S}_i| = 2^{\frac{\ell-1}{\ell}n}$
 6: for all $x \in \mathcal{S}_1 \cup \mathcal{S}_2 \cup \cdots \cup \mathcal{S}_\ell$ do
 7:     for all $k \in \{0,1\}^\kappa$ do
 8:         query $e_k(x) := \mathbf{E}(k, x, +)$
 9: for all $k' \in \{0,1\}^{\kappa'}$ do
10:     choose $\mathcal{I} \subseteq \{0,1\}^n$ s.t. $|\mathcal{I}| = t$ and $\forall x \in \mathcal{I}, \forall i \in \{1, \ldots, \ell\}$ :
          $e_{k_i}(Q_{i-1,k'}(\cdots e_{k_2}(Q_{1,k'}(e_{k_1}(Q_{0,k'}(x)))) \cdots))$ is known from line 8
11:     if $\mathcal{I}$ exists $\wedge\ \forall x \in \mathcal{I} : y(x) = Q_{\ell,k'}(e_{k_\ell}(Q_{\ell-1,k'}(\cdots e_{k_2}(Q_{1,k'}(e_{k_1}(Q_{0,k'}(x)))) \cdots)))$ then
12:         return 1
13: return 0
```

Fig. 6. Distinguisher $\mathbf{D}$ for the proof of Theorem 3.

where all keys k_i are determined by k' and $Q_{i,k'}$ is a fixed permutation for all $(i, k') \in \{0, \ldots, \ell\} \times \{0,1\}^{\kappa'}$. Again, we let $\mathsf{C}^{\mathbf{E}}_{K'}$ be the system that first chooses a uniformly random (secret) key $K' \in \{0,1\}^{\kappa'}$ and then gives access to the permutation $\mathsf{C}^{\mathbf{E}}(K', \cdot)$ in both directions (i.e., takes inputs from $\{0,1\}^n \times \{+,-\}$).

The attack on a class of so-called injective 2-query constructions given in [17] can be generalized to sequential ℓ-query constructions for arbitrary ℓ, resulting in the statement below. Note that this attack can also be seen as a lifting of an attack presented in [10] into the ideal block-cipher setting.

Theorem 3. *Let $\mathsf{C}^{(\cdot)} \colon \{0,1\}^{\kappa'} \times \{0,1\}^n \times \{+,-\} \to \{0,1\}^n$ be a sequential ℓ-query construction. For any parameter $0 < t < 2^{n/\ell-1}$ there exists a distinguisher $\mathbf{D}$ such that*

$$\Delta^{\mathbf{D}}((\mathbf{E}, \mathsf{C}^{\mathbf{E}}_{K'}), (\mathbf{E}, \mathbf{P})) \geq 1 - 2/t - 2^{\kappa' - t(n-1)},$$

where $\mathbf{D}$ makes at most $(2t + \ell) \cdot 2^{\kappa + \frac{\ell-1}{\ell}n}$ block-cipher queries as well as 2^n forward construction queries.

Proof. The distinguisher $\mathbf{D}$ is depicted in Fig. 6, the keys k_i and permutations $Q_{i,k'}$ refer to those guaranteed to exist by the definition of a sequential construction.

The distinguisher uses a similar approach as the one considered in the proof of Theorem 1. It first evaluates the given construction (denoted $\mathbf{S}$) on all possible values $x \in \{0,1\}^n$ and then collects responses to block-cipher queries on a sufficient amount of inputs (organized in sets $\mathcal{S}_1, \ldots, \mathcal{S}_\ell$) for all possible keys $k \in \{0,1\}^\kappa$. Without issuing any further queries, $\mathbf{D}$ then tries to internally simulate the evaluation of the construction C under all possible keys $k' \in \{0,1\}^{\kappa'}$. Whenever this simulated C would issue its i-th query to $\mathbf{E}$, if the queried value is in $\mathcal{S}_i$ then $\mathbf{D}$ can continue the simulation by answering this query using the value obtained during its initial batch of block-cipher queries. It remains to show that with sufficient probability there will be a set $\mathcal{I} \subseteq \{0,1\}^n$ of size at least t

containing inputs for which the whole evaluation of the construction C can be simulated successfully in the above-described way. Upon successfully completing the simulation, $\mathbf{D}$ can compare its results to the responses obtained to its construction queries and these will most probably match only if $\mathbf{S} = \mathsf{C}^{\mathbf{E}}_{K'}$.

To analyze the probability of the existence of the set $\mathcal{I}$ (formally described on line 10), we consider the setting where $\mathbf{S} = \mathsf{C}^{\mathbf{E}}_{K'}$ and the correct key was chosen on line 9, i.e., $k' = K'$. We can again define the sets

$$\begin{aligned}
\mathcal{P}_1 &= Q^{-1}_{0,k'}(\mathcal{S}_1) \\
\mathcal{P}_2 &= Q^{-1}_{0,k'}(\mathbf{E}^{-1}_{k_1}(Q^{-1}_{1,k'}(\mathcal{S}_2))) \\
&\ \ \vdots \\
\mathcal{P}_\ell &= Q^{-1}_{0,k'}(\mathbf{E}^{-1}_{k_1}(Q^{-1}_{1,k'}(\cdots Q^{-1}_{\ell-2,k'}(\mathbf{E}^{-1}_{k_{\ell-1}}(Q^{-1}_{\ell-1,k'}(\mathcal{S}_\ell)))\cdots)))
\end{aligned}$$

where each $\mathcal{P}_i$ is the set of inputs from $\{0,1\}^n$ that get mapped to an element in $\mathcal{S}_i$ after applying the first i permutations $Q_0, \ldots, Q_{i-1}$ of the sequential construction C interleaved with the first $i-1$ encryptions. The sets $\mathcal{S}_i$ were uniformly random and so are their images under a permutation, hence we again can apply Lemma 2 to see that for $\mathcal{P} = \bigcap_{i=1}^{\ell} \mathcal{P}_i$ we have

$$\mathsf{E}(|\mathcal{P}|) = \frac{\prod_{i=1}^{\ell} |\mathcal{P}_i|}{2^{n(\ell-1)}} = \frac{\prod_{i=1}^{\ell} |\mathcal{S}_i|}{2^{n(\ell-1)}} = 2t$$

and $\mathsf{Var}(|\mathcal{P}|) \leq 2t$. Chebyshev inequality then gives us $\mathsf{P}(|\mathcal{P}| < t) \leq 2/t$ and otherwise (i.e., if $|\mathcal{P}| \geq t$) the set $\mathcal{P}$ (or any its t-element subset) will serve as the set $\mathcal{I}$ on line 10, passing the test on line 11 and making $\mathbf{D}$ output 1 in this case. Hence $\mathbf{D}(\mathbf{E}, \mathsf{C}^{\mathbf{E}}_{K'})$ outputs 1 with probability at least $1 - 2/t$. On the other hand, $\mathbf{D}(\mathbf{E}, \mathbf{P})$ outputs 1 with probability at most $2^{\kappa' - t(n-1)}$ for the same reason as in the proof of Theorem 1, concluding the proof. □

Again, a trade-off between the number of construction queries and block cipher queries is possible: an analogous attack can be mounted with a lower number m of construction queries and at most $(2t + \ell) \cdot 2^{\kappa + n - \frac{\log m}{\ell}}$ block cipher queries. Also here the construction queries can be arbitrary, resulting in a known-plaintext attack.

Acknowledgements. I would like to thank Stefano Tessaro for useful discussions and helpful feedback to earlier versions of this work.

References

1. Data encryption standard. In *In FIPS PUB 46, Federal Information Processing Standards Publication*, 1977.
2. ANSI X9.52: Triple Data Encryption Algorithm Modes of Operation, 1998.
3. FIPS PUB 46-3: Data Encryption Standard (DES). National Institute of Standards and Technology, 1999.
4. Advanced encryption standard. In *FIPS PUB 197, Federal Information Processing Standards Publication*, 2001.

5. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. National Institute of Standards and Technology, Special Publication 800-67, 2004.
6. *EMV Integrated Circuit Card Specification for Payment Systems, Book 2: Security and Key Management, v.4.2.* June 2008.
7. William Aiello, Mihir Bellare, Giovanni Di Crescenzo, and Ramarathnam Venkatesan. Security amplification by composition: The case of doubly-iterated, ideal ciphers. In *Advances in Cryptology — CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 390–407. Springer Berlin Heidelberg, 1998.
8. Elena Andreeva, Andrey Bogdanov, Yevgeniy Dodis, Bart Mennink, and John P. Steinberger. On the indifferentiability of key-alternating ciphers. Cryptology ePrint Archive, Report 2013/061, 2013. `http://eprint.iacr.org/`.
9. Mihir Bellare and Phillip Rogaway. Code-based game-playing proofs and the security of triple encryption. In *Advances in Cryptology — EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 409–426. Springer Berlin Heidelberg, 2006. Full version at `http://eprint.iacr.org/2004/331`.
10. Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Francois-Xavier Standaert, John Steinberger, and Elmar Tischhauser. Key-alternating ciphers in a provable setting: encryption using a small number of public permutations. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology — EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 45–62. Springer Berlin Heidelberg, 2012.
11. W. Diffie and M. E. Hellman. Exhaustive Cryptanalysis of the NBS Data Encryption Standard. *Computer*, 10(6):74–84, 1977.
12. Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Efficient dissection of composite problems, with applications to cryptanalysis, knapsacks, and combinatorial search problems. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology — CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 719–740. Springer Berlin Heidelberg, 2012.
13. S. Even and O. Goldreich. On the power of cascade ciphers. *ACM Trans. Comput. Syst.*, 3(2):108–116, 1985.
14. Shimon Even and Yishay Mansour. A construction of a cipher from a single pseudorandom permutation. In *Journal of Cryptology*, pages 151–161. Springer Berlin Heidelberg, 1991.
15. Peter Gaži and Ueli Maurer. Cascade encryption revisited. In M. Matsui, editor, *Advances in Cryptology — ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 37–51. Springer Berlin Heidelberg, December 2009.
16. Peter Gaži and Ueli Maurer. Free-start distinguishing: Combining two types of indistinguishability amplification. In K. Kurosawa, editor, *The 4th International Conference on Information Theoretic Security - ICITS 2009*, volume 5973 of *Lecture Notes in Computer Science*, pages 28–44. Springer Berlin Heidelberg, 2010.
17. Peter Gaži and Stefano Tessaro. Efficient and optimally secure key-length extension for block ciphers via randomized cascading. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology — EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 63–80. Springer Berlin Heidelberg, 2012.
18. Joe Kilian and Phillip Rogaway. How to Protect DES Against Exhaustive Key Search (an Analysis of DESX). *Journal of Cryptology*, 14:17–35, 2001.
19. Rodolphe Lampe, Jacques Patarin, and Yannick Seurin. An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher. To appear at ASIACRYPT 2012, 2012.
20. Stefan Lucks. Attacking triple encryption. In Serge Vaudenay, editor, *Fast Software Encryption*, volume 1372 of *Lecture Notes in Computer Science*, pages 239–253. Springer Berlin Heidelberg, 1998.
21. Ueli Maurer. Indistinguishability of random systems. In Lars Knudsen, editor, *Advances in Cryptology — EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 110–132. Springer Berlin Heidelberg, May 2002.
22. Ueli Maurer and James L. Massey. Cascade ciphers: The importance of being first. *Journal of Cryptology*, 6(1):55–61, 1993.
23. Ueli Maurer and Krzysztof Pietrzak. Composition of random systems: When two weak make one strong. In Moni Naor, editor, *Theory of Cryptography — TCC 2004*, volume 2951 of *Lecture Notes in Computer Science*, pages 410–427. Springer Berlin Heidelberg, February 2004.
24. Ueli Maurer, Krzysztof Pietrzak, and Renato Renner. Indistinguishability amplification. In Alfred Menezes, editor, *Advances in Cryptology — CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 130–149. Springer Berlin Heidelberg, August 2007.

25. Ueli Maurer and Stefano Tessaro. Computational indistinguishability amplification: Tight product theorems for system composition. In Shai Halevi, editor, *Advances in Cryptology — CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 350–368. Springer Berlin Heidelberg, August 2009.
26. John Steinberger. Improved Security Bounds for Key-Alternating Ciphers via Hellinger Distance. Cryptology ePrint Archive, Report 2012/481, 2012. http://eprint.iacr.org/.
27. Stefano Tessaro. Security amplification for the cascade of arbitrarily weak PRPs: Tight bounds via the interactive Hardcore Lemma. In *Theory of Cryptography — TCC 2011*, volume 6597 of *Lecture Notes in Computer Science*, pages 37–54. Springer Berlin Heidelberg, 2011.
28. Serge Vaudenay. Decorrelation: a theory for block cipher security. *Journal of Cryptology*, 16(4):249–286, 2003.

A Intersections of Random Subsets

The following lemma is a generalization of Lemma 6 given in the full version of [17] and is used in our proofs. Let E, Var and Cov denote the usual notions of expected value, variance and covariance, respectively.

Lemma 2. *Let $\mathcal{U}$ be a set such that $|\mathcal{U}| = N$ and for $m \in \mathbb{N}$ let $\mathcal{A}_1, \cdots, \mathcal{A}_m$ be sets of size $a_1, \ldots, a_m$ respectively, such that each A_i for $i \geq 2$ is chosen independently uniformly at random from all subsets of $\mathcal{U}$ having a_i elements; A_1 may be chosen arbitrarily. If the random variable X denotes the number of elements of the intersection $\mathcal{A}_1 \cap \cdots \cap \mathcal{A}_m$ then we have $\mathsf{E}(X) = (\prod_{i=1}^m a_i)/N^{m-1}$ and $\mathsf{Var}(X) \leq (\prod_{i=1}^m a_i)/N^{m-1}$.*

Proof. It is easy to see that X can be expressed as $\sum_{i=1}^{a_1} X_i$ where X_i is the indicator random variable equal to 1 iff $e_i \in \mathcal{A}_2 \cap \cdots \cap \mathcal{A}_m$ (e_i being the i-th element of $\mathcal{A}_1$ in some ordering). For the expected value we clearly have $\mathsf{E}(X_i) = \prod_{i=2}^m (a_i/N)$ due to the independent random choice of the sets $\mathcal{A}_2, \ldots, \mathcal{A}_m$. By linearity of expectation this gives us $\mathsf{E}(X) = \sum_{i=1}^{a_1} \mathsf{E}(X_i) = (\prod_{i=1}^m a_i)/N^{m-1}$. We then obtain the variance as

$$\mathsf{Var}(X) = \sum_{i=1}^{a_1} \mathsf{Var}(X_i) + 2 \cdot \sum_{1 \leq i < j \leq a_1} \mathsf{Cov}(X_i, X_j)$$

and by bounding the terms in this equation by

$$\mathsf{Var}(X_i) = \mathsf{E}(X_i^2) - (\mathsf{E}(X_i))^2 = \prod_{i=2}^m \frac{a_i}{N} - \left(\prod_{i=2}^m \frac{a_i}{N}\right)^2 \leq \frac{\prod_{i=2}^m a_i}{N^{m-1}}$$
$$\mathsf{Cov}(X_i, X_j) = \mathsf{E}(X_i \cdot X_j) - \mathsf{E}(X_i) \cdot \mathsf{E}(X_j) < 0$$

we obtain the desired result. □

B Security of Key-Alternating Ciphers

In this appendix we present several bounds recently proved for the security of key-alternating ciphers in the random-permutation model, recast into our formalism.

Theorem 4. *Let $\mathsf{A}_{\ell,\bar{Z}}$ denote the key-alternating cipher of length ℓ as described above.*

1. *[10] For any $q < 2^n/100$ we have*

$$\Delta_q((\bar{\mathbf{P}}_2, \mathsf{A}_{2,\bar{Z}}^{\bar{\mathbf{P}}_2}), \bar{\mathbf{P}}_3) \leq \frac{8.6q^3}{2^{2n}} + \frac{3q^2}{2^{\frac{4}{3}n}}.$$

2. *[26] For any $\ell \geq 1$ and $q < 2^n/100$ we have*

$$\Delta_q((\bar{\mathbf{P}}_\ell, \mathsf{A}_{\ell,\bar{Z}}^{\bar{\mathbf{P}}_\ell}), \bar{\mathbf{P}}_{\ell+1}) \leq 3\ell \cdot \frac{q^2}{2^{\frac{3}{2}n}} + (\ell+1) \cdot \frac{q^\ell}{2^{\frac{\ell^2}{\ell+1}n}}.$$

3. *[19] For any even $\ell \geq 1$ we have*

$$\Delta_q((\bar{\mathbf{P}}_\ell, \mathsf{A}_{\ell,\bar{Z}}^{\bar{\mathbf{P}}\ell}), \bar{\mathbf{P}}_{\ell+1}) \leq 2^{\frac{\ell}{4}+3} \cdot \left(\frac{q^{\ell+2}}{2^{\ell n}}\right)^{\frac{1}{4}}.$$