# Security Amplification for the Composition of Block Ciphers: Simpler Proofs and New Results

Benoit Cogliati[1], Jacques Patarin[1], and Yannick Seurin[2(✉)]

[1] University of Versailles, Versailles, France
benoit.cogliati@ens.uvsq.fr, jacques.patarin@uvsq.fr
[2] ANSSI, Paris, France
yannick.seurin@m4x.org

**Abstract.** Security amplification results for block ciphers typically state that cascading (i.e., composing with independent keys) two (or more) block ciphers yields a new block cipher that offers better security against some class of adversaries and/or that resists stronger adversaries than each of its components. One of the most important results in this respect is the so-called "two weak make one strong" theorem, first established up to logarithmic terms by Maurer and Pietrzak (TCC 2004), and later optimally tightened by Maurer, Pietrzak, and Renner (CRYPTO 2007), which states that, in the information-theoretic setting, cascading $F$ and $G^{-1}$, where $F$ and $G$ are respectively $(q, \varepsilon_F)$-secure and $(q, \varepsilon_G)$-secure against non-adaptive chosen-plaintext (NCPA) attacks, yields a block cipher which is $(q, \varepsilon_F + \varepsilon_G)$-secure against adaptive chosen-plaintext and ciphertext (CCA) attacks. The first contribution of this work is a surprisingly simple proof of this theorem, relying on Patarin's H-coefficient method. We then extend our new proof to obtain new results (still in the information-theoretic setting). In particular, we prove a new composition theorem (which can be seen as the generalization of the "two weak make one strong" theorem to the composition of $n > 2$ block ciphers) which provides both amplification of the advantage and strengthening of the distinguisher's class in some optimal way (indeed we prove that our new composition theorem is tight up to some constant).

**Keywords:** Block cipher · Security amplification · Cascade · Composition · Provable security

## 1 Introduction

Security Amplification for Block Ciphers. The usual security notion for a block cipher $E$ is *pseudorandomness*, which measures the (in-)ability of

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


A. Joux and A. Youssef (Eds.): SAC 2014, LNCS 8781, pp. 129–146, 2014.
DOI: 10.1007/978-3-319-13051-4_8

an adversary (the *distinguisher*) which is given oracle access to a permutation (and potentially its inverse) to tell whether it is interacting with the block cipher $E_K$ for some randomly drawn key $K$ or with a truly random permutation. One usually classifies distinguishers according to the way they can issue their queries. A distinguisher which can only make direct (plaintext) queries to the permutation oracle is called a CPA-distinguisher, whereas it is called a CCA-distinguisher when it can make both direct and inverse (ciphertext) queries. Both types come in a non-adaptive variant (NCPA and NCCA respectively), i.e., the adversary must choose all its queries before receiving any answer from the permutation oracle. A block cipher is said to be $(q, \varepsilon)$-ATK secure when no distinguisher in the attack class ATK (for instance NCPA, etc.) making at most $q$ oracle queries can distinguish $E_K$ from a truly random permutation with advantage better than $\varepsilon$.

The security amplification problem is to determine whether adequately combining some mildly secure block ciphers $E_1, \ldots, E_n$ can yield a block cipher $F$ with stronger security guarantees than each of its components. (This question naturally extends to other cryptographic primitives such as pseudorandom generators or pseudorandom functions, but in this paper we focus on pseudorandom permutations, i.e., block ciphers.) Here, "stronger" security guarantees might mean either that $F$ has a smaller distinguishing advantage in face of some fixed class of distinguishers than each component $E_i$ (something we will informally refer to as *$\varepsilon$-amplification*), or that $F$ can withstand attacks from a stronger class of adversaries than each of its components (something we will call *class-amplification*). We clarify this distinction with a prominent example of each type of result.

The classical example of an $\varepsilon$-amplification result states that cascading two block ciphers $F$ and $G$ which are respectively $(q, \varepsilon_F)$- and $(q, \varepsilon_G)$-NCPA (resp. CPA) secure yields a block cipher which is $(q, 2\varepsilon_F\varepsilon_G)$-NCPA (resp. CPA) secure. Hence, when $\varepsilon_F, \varepsilon_G < 1/2$, the new block cipher is indeed strictly more secure than each of its components. This was proved (in the information-theoretic setting, i.e., when considering computationally unbounded adversaries) by Vaudenay (see [Vau98] for the non-adaptive case and [Vau99] for the adaptive case) using the *decorrelation theory* framework [Vau03]. (See also [KNR09, Theorem 3.8] for a different proof for self-composition in the non-adaptive case.) A computational analogue of this result was later proved by Maurer and Tessaro [MT09].

For the class-amplification type of results, one of the most notable examples is what we will refer to as the "two weak make one strong" (*2W1S* for short) theorem, which states that if $F$ and $G$ are resp. $(q, \varepsilon_F)$- and $(q, \varepsilon_G)$-NCPA secure, then the composition $G^{-1} \circ F$ is $(q, \varepsilon_F + \varepsilon_G)$-CCA secure (a result which is tight in general). Note that here, the resulting cipher withstands much stronger attacks than each component $F$ and $G$, but its CCA advantage is strictly larger than each of the NCPA advantages of $F$ and $G$. This theorem was first proved up to logarithmic terms by Maurer and Pietrzak [MP04], while the tight version was later proved by Maurer, Pietrzak, and Renner [MPR07]

using the framework of random systems [Mau02]. We stress that this result only holds in the information-theoretic setting. In the computational setting, the composition of non-adaptively secure block ciphers does not, in general, yield an adaptively secure one [Mye04, Pie05a], though some partial positive results are known [LR86, Pie06].

Our Contribution. The starting point of our work is a surprisingly simple proof of the 2W1S theorem. Our new technique relies on simple manipulations of transition probabilities (which are nothing else, up to some normalization factors, than the H-coefficients of Patarin [Pat08]) and eschews completely the heavy machinery of the random systems framework [Mau02] on which the only previously known proof was based [MPR07]. We think that having an elementary proof of an important result (on which a number of subsequent papers rely, notably in coupling-based security proofs [MRS09, HR10, LPS12, LS14]) is an interesting contribution in itself. To emphasize our point, we stress that a crucial lemma of the random systems framework (namely Theorem 2 of [Mau02]), to which the proof of the 2W1S theorem of [MPR07] appeals, was later found to be incorrectly stated (and also that the only known proof of this lemma in [Pie05b] was flawed) by Jetchev *et al.* [JÖS12]. Hence, the 2W1S theorem can only be considered formally proven by combining results from three different papers [Mau02, MPR07, JÖS12], a somehow unsatisfying state of affairs.

Motivated by our findings, we consider the following problem: given three (or more) block ciphers which are $(q, \varepsilon)$-NCPA secure, can we get both $\varepsilon$-amplification *and* class-amplification at the same time, i.e., a composed block cipher which is $(q, \varepsilon')$-CCA secure for $\varepsilon' < \varepsilon$, in some optimal manner?[1] Focusing on self-composition for simplicity, consider a block cipher $E$ such that both $E$ and $E^{-1}$ are $(q, \varepsilon)$-NCPA secure.[2] What can we say about the CCA-security of the $n$-fold composition $E^n$? Using known results, a straightforward answer (assuming $n$ even) can be obtained by first (recursively) applying the $\varepsilon$-amplification theorem for NCPA-secure block ciphers to each half of the cascade, thereby getting

$$\mathbf{Adv}^{\mathrm{ncpa}}_{E^{n/2}}(q) \leq 2^{\frac{n}{2}-1}\varepsilon^{\frac{n}{2}} \qquad \text{and} \qquad \mathbf{Adv}^{\mathrm{ncpa}}_{(E^{n/2})^{-1}}(q) \leq 2^{\frac{n}{2}-1}\varepsilon^{\frac{n}{2}},$$

and then the 2W1S theorem to obtain

$$\mathbf{Adv}^{\mathrm{cca}}_{E^n}(q) \leq \mathbf{Adv}^{\mathrm{ncpa}}_{E^{n/2}}(q) + \mathbf{Adv}^{\mathrm{ncpa}}_{(E^{n/2})^{-1}}(q) \leq (2\varepsilon)^{\frac{n}{2}}.$$

For $n$ odd, a similar reasoning yields (by cutting $E^n$ into two unbalanced halves)

$$\mathbf{Adv}^{\mathrm{cca}}_{E^n}(q) \leq \mathbf{Adv}^{\mathrm{ncpa}}_{E^{(n+1)/2}}(q) + \mathbf{Adv}^{\mathrm{ncpa}}_{(E^{(n-1)/2})^{-1}}(q) \leq 2^{\frac{n-1}{2}}\varepsilon^{\frac{n+1}{2}} + 2^{\frac{n-3}{2}}\varepsilon^{\frac{n-1}{2}}.$$

[1] This requires at least three block ciphers since the 2W1S theorem is tight. Hence, in general, from two $(q, \varepsilon)$-NCPA secure block ciphers $F$ and $G$, one can at best obtain a $(q, 2\varepsilon)$-CCA secure one.

[2] A larger number of block cipher designs have similar provable security in the direct and inverse direction because of their involution-like structure, for example balanced Feistel schemes.

In particular, for $n = 3$, the best one can prove from previous results is that

$$\mathbf{Adv}^{\mathrm{cca}}_{E^3} \leq \varepsilon + 2\varepsilon^2.$$

Hence, one gets (provable) $\varepsilon$-amplification only for $n \geq 4$, assuming $\varepsilon < 1/4$.

In this paper, we prove that the CCA-security of $E^n$ is actually much better, namely

$$\mathbf{Adv}^{\mathrm{cca}}_{E^n}(q) \leq (2\varepsilon)^{n-1}.$$

Hence, for $n \geq 3$, this provides both $\varepsilon$-amplification *and* class-amplification as soon as

$$\varepsilon < \frac{1}{2 \cdot 2^{1/(n-2)}}$$

(hence, in particular as soon as $\varepsilon < 1/4$ for any $n \geq 3$). In fact we prove a more general theorem (see Theorem 2) which also implies the following interesting corollary. Let $E$, $F$, $G$ be three block ciphers such that $E$, $F$, $F^{-1}$ and $G^{-1}$ are $(q, \varepsilon)$-NCPA secure. Then the composition $G \circ F \circ E$ is $(q, 4\varepsilon^2)$-CCA secure.

A Word of Interpretation. Our new result has some interesting implications regarding the superiority of triple- versus double-encryption. This fact has already been widely analyzed in the ideal cipher model [ABCV98,BR06]. Our new theorem may be seen as yet another expression of this phenomenon in the standard, information-theoretic setting. For concreteness, assume that we have at hand a block cipher $E$ such that $E$ and $E^{-1}$ are only, say, $(2^{40}, 2^{-30})$-NCPA secure, a mild security insurance by current standards. Using double-encryption, one "restores" NCPA-security (since $E^2$ and $(E^2)^{-1}$ are ensured to be $(2^{40}, 2^{-59})$-NCPA secure) but in general one cannot exclude that a CCA-attack will break $E^2$ with $2^{40}$ queries and advantage $2^{-30}$. On the other hand, triple-encryption is good enough here, since our new result shows that $E^3$ is $(2^{40}, 2^{-58})$-CCA secure.

Related Work. The topic of security amplification is too broad to be entirely covered here. Restricting our attention to block cipher security amplification, we mention that a long line of work considered provable security results for cascade encryption *in the ideal cipher model* [ABCV98,BR06,GM09,Lee13], which is quite orthogonal to our setting: working in the ideal cipher model is in some sense equivalent to upper bounding the knowledge of the adversary on the underlying block cipher(s) (since it can only make a limited number of ideal cipher queries), whereas we consider computationally unbounded adversaries, in the standard, non-idealized model (in particular, the adversary has complete knowledge of the underlying block cipher(s), and may, e.g., represent them as a huge look-up table).

Organization. We start with useful definitions and the necessary background on transition probabilities and how these quantities are related to the advantage against different classes of distinguishers in Sect. 2. In Sect. 3, we give our new and substantially simpler proof of the 2W1S theorem. Then, in Sect. 4, we

extend this result to the general case of the composition of $n \geq 2$ non-adaptively secure block ciphers (we treat the special case $n = 3$ in the full version of the paper [CPS14]). Finally, in Sect. 5, we show that our new result is tight up to some constant.

## 2 Preliminaries

### 2.1 Notation and Definitions

Given a non-empty set $S$, the set of all permutations of $S$ is denoted $\mathsf{Perm}(S)$. We write $s \leftarrow_{\$} S$ to mean that a value is sampled uniformly at random from $S$ and assigned to $s$.

**Definition 1 (Statistical Distance).** *Let $\Omega$ be a finite event space and let $\mu$ and $\nu$ be two probability distributions defined on $\Omega$. The* statistical distance *(or total variation distance) between $\mu$ and $\nu$, denoted $\|\mu - \nu\|$ is defined as:*

$$\|\mu - \nu\| = \frac{1}{2} \sum_{\omega \in \Omega} |\mu(\omega) - \nu(\omega)|.$$

The following definitions can easily be seen equivalent:

$$\|\mu - \nu\| = \max_{S \subseteq \Omega} \{\mu(S) - \nu(S)\} = \max_{S \subseteq \Omega} \{\nu(S) - \mu(S)\} = \max_{S \subseteq \Omega} \{|\mu(S) - \nu(S)|\}.$$

Composition of Block Ciphers. Let $\mathcal{M}$ and $\mathcal{K}$ be two sets. A block cipher with message space $\mathcal{M}$ and key space $\mathcal{K}$ is a mapping $E : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ such that for any $K \in \mathcal{K}$, the partial mapping $E(K, \cdot)$ is a permutation of $\mathcal{M}$. We interchangeably use the notation $E_K(x)$ for $E(K, x)$, the inverse of $E_K$ being denoted $E_K^{-1}$. Given two block ciphers $E$ and $F$ with the same message space $\mathcal{M}$ and respective key spaces $\mathcal{K}_E$ and $\mathcal{K}_F$, we denote $F \circ E$ the block cipher with message space $\mathcal{M}$ and key space $\mathcal{K}_E \times \mathcal{K}_F$ defined as

$$F \circ E_{(K_E, K_F)}(x) = F_{K_F}(E_{K_E}(x)).$$

We call $F \circ E$ interchangeably the *composition* or the *cascade* of $E$ and $F$. This definition extends straightforwardly to the composition of $n > 2$ block ciphers. We denote $E^n$ the $n$-fold self-composition of $E$ (with independent keys).

### 2.2 Security Definitions and Classical Lemmas

Fix some message space $\mathcal{M}$ and denote $M = |\mathcal{M}|$. We denote $(\mathcal{M})_q$ the set of all $q$-tuple of pairwise distinct elements of $\mathcal{M}$. Let $E$ be a block cipher with message space $\mathcal{M}$ and key space $\mathcal{K}_E$. Given an integer $q \geq 1$ and two $q$-tuples $x = (x_1, \ldots, x_q) \in (\mathcal{M})_q$ and $y = (y_1, \ldots, y_q) \in (\mathcal{M})_q$ of pairwise distinct elements of $\mathcal{M}$, we denote

$$\mathsf{p}_E(x, y) = \Pr\left[K \leftarrow_{\$} \mathcal{K}_E : E_K(x) = y\right] = \frac{|\{K \in \mathcal{K}_E : E_K(x) = y\}|}{|\mathcal{K}_E|},$$

where the notation $E_K(x) = y$ is a shorthand meaning that $E_K(x_i) = y_i$ for all $1 \leq i \leq q$. We also denote

$$\mathsf{p}^* = \Pr\left[P \leftarrow_\$ \mathsf{Perm}(\mathcal{M}) : P(x) = y\right] = \frac{1}{M(M-1)\cdots(M-q+1)}.$$

When $x$ is fixed,

$$\mathsf{p}_{E,x} : y \mapsto \mathsf{p}_E(x, y)$$

is the probability distribution (over the choice of a uniformly random key $K \leftarrow_\$ \mathcal{K}_E$) of the $q$-tuple of ciphertexts when $E$ receives the $q$-tuple of plaintexts $x$. Similarly, when $y$ is fixed,

$$\mathsf{p}_{E^{-1},y} : x \mapsto \mathsf{p}_E(x, y)$$

is the probability distribution of the $q$-tuples of plaintexts when $E^{-1}$ receives the $q$-tuple of ciphertexts $y$. Overloading the notation, $\mathsf{p}^*$ will also denote the uniform probability distribution over $(\mathcal{M})_q$. Note that for any $x = (x_1, \ldots, x_q) \in (\mathcal{M})_q$ and any $y = (y_1, \ldots, y_q) \in (\mathcal{M})_q$,

$$\sum_{z \in (\mathcal{M})_q} (\mathsf{p}_E(x, z) - p^*) = \sum_{z \in (\mathcal{M})_q} (\mathsf{p}_E(z, y) - p^*) = 0. \tag{1}$$

Let $\mathcal{D}$ be a distinguisher with (potentially two-sided) oracle access to some permutation $P \in \mathsf{Perm}(\mathcal{M})$, whose goal is to distinguish whether it is interacting with $E_K(\cdot)$ for some random key $K \leftarrow_\$ \mathcal{K}$, or with a uniformly random permutation $P \leftarrow_\$ \mathsf{Perm}(\mathcal{M})$. We classify distinguishers according to the type of attacks they can perform:

- chosen-plaintext attacks (CPA), where $\mathcal{D}$ can only make direct (i.e., plaintext) queries to the permutation oracle,
- and chosen-plaintext and ciphertext attacks (CCA), where $\mathcal{D}$ can make both direct and inverse (i.e., ciphertext) queries to the permutation oracle.

Additionally, we also consider the non-adaptive variants of these two types of attacks, namely NCPA and NCCA, where the distinguisher must choose all its queries before receiving any answer from the permutation oracle. We consider computationally unbounded distinguishers, and we assume *wlog* that the distinguisher is deterministic and never makes redundant queries.

The distinguishing advantage of $\mathcal{D}$ is defined as

$$\mathbf{Adv}(\mathcal{D}) = \left|\Pr\left[K \leftarrow_\$ \mathcal{K} : \mathcal{D}^{E_K} = 1\right] - \Pr\left[P \leftarrow_\$ \mathsf{Perm}(\mathcal{M}) : \mathcal{D}^{P} = 1\right]\right|,$$

where, depending on the type of the distinguisher, $\mathcal{D}$ can make one-sided or two-sided queries to the permutation oracle. For $q$ a non-negative integer, the insecurity (or advantage) of $E$ against ATK-attacks, where ATK $\in \{$(N)CPA, (N)CCA$\}$ is defined as

$$\mathbf{Adv}^{\mathrm{atk}}_E(q) = \max_{\mathcal{D}} \mathbf{Adv}(\mathcal{D}),$$

where the maximum is taken over all distinguishers $\mathcal{D}$ of type ATK making at most $q$ oracle queries. We say that $E$ is $(q,\varepsilon)$-ATK secure if $\mathbf{Adv}_E^{\mathrm{atk}}(q) \leq \varepsilon$.

Our analysis will rely on the H-coefficient method, first introduced by Patarin to prove the strong pseudorandomness of the 4-round Feistel scheme [Pat90, Pat91, Pat08]. We recall the two fundamental results of the H-coefficient method, regarding NCPA and CCA distinguishers respectively. For completeness, we give a proof of these results in Appendix A.

**Lemma 1 (NCPA security).** *Let $E$ be a block cipher with message space $\mathcal{M}$. Then*

$$\mathbf{Adv}_E^{\mathrm{ncpa}}(q) = \max_{x \in (\mathcal{M})_q} \|\mathsf{p}_{E,x} - \mathsf{p}^*\|.$$

**Lemma 2 (CCA security).** *Let $E$ be a block cipher with message space $\mathcal{M}$. Assume that there exists $\varepsilon$ such that for any $q$-tuples $x, y \in (\mathcal{M})_q$, one has*

$$\mathsf{p}_E(x,y) \geq (1-\varepsilon)\mathsf{p}^*.$$

*Then*

$$\mathbf{Adv}_E^{\mathrm{cca}}(q) \leq \varepsilon.$$

## 3 A Simple Proof of the "Two Weak Make One Strong" Theorem

In this section, we derive in a straightforward manner the "two weak make one strong" theorem [MP04, MPR07]. We start by giving a handful expression for the quantity $\mathsf{p}_{F\circ E}(x,y)$.

**Lemma 3.** *Let $E$ and $F$ be two block ciphers with the same message space $\mathcal{M}$ and respective key spaces $\mathcal{K}_E$ and $\mathcal{K}_F$. Then for any $q$-tuples $x$ and $y$ of pairwise distinct elements of $\mathcal{M}$, one has*

$$\mathsf{p}_{F\circ E}(x,y) = \mathsf{p}^* + \sum_{z \in (\mathcal{M})_q} (\mathsf{p}_E(x,z) - \mathsf{p}^*)(\mathsf{p}_F(z,y) - \mathsf{p}^*). \tag{2}$$

*Proof.* One has

$$\begin{aligned}
\mathsf{p}_{F\circ E}(x,y) &= \sum_{z \in (\mathcal{M})_q} \mathsf{p}_E(x,z)\mathsf{p}_F(z,y) \\
&= \sum_z (\mathsf{p}_E(x,z) - \mathsf{p}^* + \mathsf{p}^*)(\mathsf{p}_F(z,y) - \mathsf{p}^* + \mathsf{p}^*) \\
&= \sum_z (\mathsf{p}_E(x,z) - \mathsf{p}^*)(\mathsf{p}_F(z,y) - \mathsf{p}^*) \\
&\quad + \mathsf{p}^* \underbrace{\sum_z (\mathsf{p}_E(x,z) - \mathsf{p}^*)}_{=0 \text{ by (1)}} + \mathsf{p}^* \underbrace{\sum_z (\mathsf{p}_F(z,y) - \mathsf{p}^*)}_{=0 \text{ by (1)}} + \underbrace{\sum_z (\mathsf{p}^*)^2}_{=\mathsf{p}^*} \\
&= \mathsf{p}^* + \sum_z (\mathsf{p}_E(x,z) - \mathsf{p}^*)(\mathsf{p}_F(z,y) - \mathsf{p}^*),
\end{aligned}$$

from which the result follows. □

The next step is to lower bound the sum appearing in the right hand-side of (2). Note that this term is exactly a covariance term. In particular, one could use the Cauchy-Schwarz inequality to get

$$\left|\sum_{z\in(\mathcal{M})_q}(\mathsf{p}_E(x,z)-\mathsf{p}^*)(\mathsf{p}_F(z,y)-\mathsf{p}^*)\right| \leq \sqrt{\sum_{z\in(\mathcal{M})_q}(\mathsf{p}_E(x,z)-\mathsf{p}^*)^2}\sqrt{\sum_{z\in(\mathcal{M})_q}(\mathsf{p}_F(z,y)-\mathsf{p}^*)^2}.$$

However, the quantities appearing in the right hand-side involve the Euclidean distance between $\mathsf{p}_{E,x}$ (resp. $\mathsf{p}_{F^{-1},y}$) and $\mathsf{p}^*$, which to the best of our knowledge is not related to any standard attack. Hence we prove in the next lemma a different bound which involves the statistical distance instead, which, as recalled in Lemma 1, is related to NCPA attacks.

**Lemma 4.** *Let $E$ and $F$ be two block ciphers with the same message space $\mathcal{M}$ and respective key spaces $\mathcal{K}_E$ and $\mathcal{K}_F$. Then for any $q$-tuples $x$ and $y$ of pairwise distinct elements of $\mathcal{M}$, one has*

$$\sum_{z\in(\mathcal{M})_q}(\mathsf{p}_E(x,z)-\mathsf{p}^*)(\mathsf{p}_F(z,y)-\mathsf{p}^*) \geq -\mathsf{p}^*\left(\|\mathsf{p}_{E,x}-\mathsf{p}^*\|+\|\mathsf{p}_{F^{-1},y}-\mathsf{p}^*\|\right).$$

*Proof.* Let

$$S \stackrel{\text{def}}{=} \sum_{z\in(\mathcal{M})_q}(\mathsf{p}_E(x,z)-\mathsf{p}^*)(\mathsf{p}_F(z,y)-\mathsf{p}^*) = \sum_{z\in(\mathcal{M})_q}(\mathsf{p}_{E,x}(z)-\mathsf{p}^*)(\mathsf{p}_{F^{-1},y}(z)-\mathsf{p}^*).$$

To simplify notation, we rename the probability distributions as $\mu := \mathsf{p}_{E,x}$ and $\nu := \mathsf{p}_{F^{-1},y}$. Then, keeping only the negative terms in the sum, we have

$$\begin{aligned}
S &\geq \sum_{z\in(\mathcal{M})_q:\begin{cases}\mu(z)>\mathsf{p}^*\\ \nu(z)<\mathsf{p}^*\end{cases}}(\mu(z)-\mathsf{p}^*)(\nu(z)-\mathsf{p}^*) \\
&\qquad + \sum_{z\in(\mathcal{M})_q:\begin{cases}\mu(z)<\mathsf{p}^*\\ \nu(z)>\mathsf{p}^*\end{cases}}(\mu(z)-\mathsf{p}^*)(\nu(z)-\mathsf{p}^*) \\
&\geq \sum_{z\in(\mathcal{M})_q:\begin{cases}\mu(z)>\mathsf{p}^*\\ \nu(z)<\mathsf{p}^*\end{cases}}(\mu(z)-\mathsf{p}^*)(-\mathsf{p}^*) + \sum_{z\in(\mathcal{M})_q:\begin{cases}\mu(z)<\mathsf{p}^*\\ \nu(z)>\mathsf{p}^*\end{cases}}(-\mathsf{p}^*)(\nu(z)-\mathsf{p}^*) \\
&= -\mathsf{p}^*\left(\sum_{z\in(\mathcal{M})_q:\begin{cases}\mu(z)>\mathsf{p}^*\\ \nu(z)<\mathsf{p}^*\end{cases}}(\mu(z)-\mathsf{p}^*) + \sum_{z\in(\mathcal{M})_q:\begin{cases}\mu(z)<\mathsf{p}^*\\ \nu(z)>\mathsf{p}^*\end{cases}}(\nu(z)-\mathsf{p}^*)\right) \\
&\geq -\mathsf{p}^*(\|\mu-\mathsf{p}^*\|+\|\nu-\mathsf{p}^*\|),
\end{aligned}$$

where for the last inequality we used that

$$\|\mu - \mathsf{p}^*\| = \max_{S \subseteq (\mathcal{M})_q} \sum_{z \in S} (\mu(z) - \mathsf{p}^*)$$

(and the analogue equality for $\nu$). This proves the result. □

We can finally prove the "two weak make one strong" composition theorem.

**Theorem 1.** *Let $E$ and $F$ be two block ciphers with the same message space $\mathcal{M}$. For any integer $q$, one has*

$$\mathbf{Adv}^{\mathrm{cca}}_{F \circ E}(q) \leq \mathbf{Adv}^{\mathrm{ncpa}}_{E}(q) + \mathbf{Adv}^{\mathrm{ncpa}}_{F^{-1}}(q).$$

*Proof.* Fix any $q$-tuples $x, y \in (\mathcal{M})_q$. Then

$$\begin{aligned}
\mathsf{p}_{F \circ E}(x, y) &= \mathsf{p}^* + \sum_{z \in (\mathcal{M})_q} (\mathsf{p}_E(x, z) - \mathsf{p}^*)(\mathsf{p}_F(z, y) - \mathsf{p}^*) && \text{(Lemma 3)} \\
&\geq \mathsf{p}^* - \mathsf{p}^* \left( \|\mathsf{p}_{E,x} - \mathsf{p}^*\| + \|\mathsf{p}_{F^{-1},y} - \mathsf{p}^*\| \right) && \text{(Lemma 4)} \\
&\geq \mathsf{p}^*(1 - \mathbf{Adv}^{\mathrm{ncpa}}_{E}(q) - \mathbf{Adv}^{\mathrm{ncpa}}_{F^{-1}}(q)). && \text{(Lemma 1)}
\end{aligned}$$

The result follows by Lemma 2. □

To illustrate the usefulness of Eq. (2), we give a simple proof of the $\varepsilon$-amplification theorem for NCPA-secure ciphers [Vau98], as well as an amplification theorem for security against known-plaintext attacks (KPA), in the full version of this paper [CPS14].

## 4 Many Weak Make One Even Stronger

Let $n \geq 1$ be an integer. In this section, we extend Theorem 1 to the composition of $n$ block ciphers (the special case $n = 3$ is treated in details in the full version of this paper [CPS14]).

We start by generalizing Lemma 3.

**Lemma 5.** *Let $E_1, \ldots, E_n$ be $n$ block ciphers with the same message space $\mathcal{M}$. Then for any $q$-tuples $x$ and $y$ of pairwise distinct elements of $\mathcal{M}$, one has*

$$\mathsf{p}_{E_n \circ \cdots \circ E_1}(x, y) = \mathsf{p}^* + \sum_{x_1, \ldots, x_{n-1} \in (\mathcal{M})_q} \left( \prod_{i=1}^{n} (\mathsf{p}_{E_i}(x_{i-1}, x_i) - \mathsf{p}^*) \right) \tag{3}$$

*where $x_0 := x$ and $x_n := y$.*

*Proof.* This result can be shown by induction. For $i \geq 1$, let $(\mathrm{H}_i)$ be the following proposition: for any $j \in \{1, \ldots, i\}$, for any block ciphers $E_1, \ldots, E_j$ with the same message space $\mathcal{M}$ and for any $q$-tuples $x_0$ and $x_j$ of pairwise distinct elements of $\mathcal{M}$, one has

$$\mathsf{p}_{E_j \circ \cdots \circ E_1}(x_0, x_j) = \mathsf{p}^* + \sum_{x_1,\ldots,x_{j-1} \in (\mathcal{M})_q} \left( \prod_{i=1}^{j} (\mathsf{p}_{E_i}(x_{i-1}, x_i) - \mathsf{p}^*) \right).$$

Lemma 3 corresponds to $(\mathrm{H}_2)$.

Assume that $(\mathrm{H}_k)$ holds for an integer $k \geq 2$. Let $E_1, \ldots, E_{k+1}$ be block ciphers with the same message space $\mathcal{M}$ and $x_0, x_{k+1} \in (\mathcal{M})_q$. Then

$$\begin{aligned}
&\mathsf{p}_{E_{k+1} \circ \cdots \circ E_1}(x_0, x_{k+1}) \\
&\quad = \mathsf{p}^* + \sum_{x_1 \in (\mathcal{M})_q} (\mathsf{p}_{E_1}(x_0, x_1) - \mathsf{p}^*)(\mathsf{p}_{E_{k+1} \circ \cdots \circ E_2}(x_1, x_{k+1}) - \mathsf{p}^*) && (\mathrm{H}_2) \\
&\quad = \mathsf{p}^* + \sum_{x_1 \in (\mathcal{M})_q} (\mathsf{p}_{E_1}(x_0, x_1) - \mathsf{p}^*) \sum_{\substack{x_2,\ldots,x_k \\ \in (\mathcal{M})_q}} \prod_{i=2}^{k+1} (\mathsf{p}_{E_i}(x_{i-1}, x_i) - \mathsf{p}^*) && (\mathrm{H}_k)
\end{aligned}$$

from which the result follows. □

We now have to study the sum appearing in the right hand-side of (3) in the same way as in the proof of Lemma 4, i.e., by splitting the sum according to the sign of each term of the product. In order to have a more compact notation, for a tuple $(t_0, \ldots, t_n) \in ((\mathcal{M})_q)^{n+1}$ and for each $i \in \{1, \ldots, n\}$ we denote:

- $C_{0,i}$ the inequality $\mathsf{p}_{E_i}(t_{i-1}, t_i) - \mathsf{p}* > 0$ and
- $C_{1,i}$ the inequality $\mathsf{p}_{E_i}(t_{i-1}, t_i) - \mathsf{p}* < 0$.

Then every part of the sum can be parametrized with a $n$-tuple $k = (k_1, \ldots, k_n)$ of integers in $\{0, 1\}$, the product being positive if and only if $k_1 + \ldots + k_n \equiv 0 \bmod 2$. Of course, the cases which have to be dealt carefully with are the ones where the product is negative (i.e., $k_1 + \ldots + k_n \equiv 1 \bmod 2$). This is what is done in the following lemma.

**Lemma 6.** *Let $E_1, \ldots, E_n$ be $n$ block ciphers with the same message space $\mathcal{M}$ and $k = (k_1, \ldots, k_n) \in \{0, 1\}^n$ such that $k_1 + \ldots + k_n \equiv 1 \bmod 2$. For any fixed $q$-tuples $t_0, t_n$ in $(\mathcal{M})_q$, denote*

$$A_k(t_0, t_n) := \{(t_1, \ldots, t_{n-1}) \in ((\mathcal{M})_q)^{n-1} \mid \forall i \in \{1, \ldots, n\}, C_{k_i,i} \text{ holds}\}.$$

*Then*

$$\begin{aligned}
&\sum_{t \in A_k(t_0,t_n)} \prod_{1 \leq i \leq n} (\mathsf{p}_{E_i}(t_{i-1}, t_i) - \mathsf{p}^*) \\
&\qquad \geq -\mathsf{p}^* \max_{1 \leq i \leq n} \left( \prod_{1 \leq j \leq i-1} \mathbf{Adv}^{\mathrm{ncpa}}_{E_j}(q) \times \prod_{i+1 \leq j \leq n} \mathbf{Adv}^{\mathrm{ncpa}}_{E_j^{-1}}(q) \right).
\end{aligned}$$

*Proof.* Since $k_1 + \ldots + k_n \equiv 1 \bmod 2$, one can find an index $j$ such that $k_j = 1$, i.e., $\mathsf{p}_{E_j}(t_{j-1}, t_j) - \mathsf{p}^* < 0$. Then, one has

$$\sum_{t \in A_k(t_0,t_n)} \prod_{1 \le i \le n} (\mathsf{p}_{E_i}(t_{i-1}, t_i) - \mathsf{p}^*) \ge -\mathsf{p}^* \sum_{t \in A_k(t_0,t_n)} \prod_{\substack{1 \le i \le n \\ i \ne j}} (\mathsf{p}_{E_i}(t_{i-1}, t_i) - \mathsf{p}^*).$$

In the sum appearing in the right hand-side, every term is positive since there is an even number of negative terms in each product. Hence,

$$\sum_{t \in A_k(t_0,t_n)} \prod_{1 \le i \le n} (\mathsf{p}_{E_i}(t_{i-1}, t_i) - \mathsf{p}^*) \ge -\mathsf{p}^* \sum_{t \in A_k(t_0,t_n)} \prod_{\substack{1 \le i \le n \\ i \ne j}} |\mathsf{p}_{E_i}(t_{i-1}, t_i) - \mathsf{p}^*|.$$

Let

$$B := \{(t_1, \ldots, t_{j-1}) \in ((\mathcal{M})_q)^{j-1} \mid \forall i \in \{1, \ldots, j-1\}, C_{k_i,i} \text{ holds}\} \text{ and}$$
$$C := \{(t_j, \ldots, t_{n-1}) \in ((\mathcal{M})_q)^{n-j} \mid \forall i \in \{j+1, \ldots, n\}, C_{k_i,i} \text{ holds}\}.$$

One has $A_k(t_0, t_n) \subseteq B \times C$ since the only difference between the sets is that in $B \times C$ we dropped the requirement that $C_{k_j,j}$ (i.e., inequality $\mathsf{p}_{E_j}(t_{j-1}, t_j) < \mathsf{p}^*$) holds. Hence,

$$\sum_{t \in A_k(t_0,t_n)} \prod_{1 \le i \le n} (\mathsf{p}_{E_i}(t_{i-1}, t_i) - \mathsf{p}^*) \ge -\mathsf{p}^* \sum_{t \in B \times C} \prod_{\substack{1 \le i \le n \\ i \ne j}} |\mathsf{p}_{E_i}(t_{i-1}, t_i) - \mathsf{p}^*|$$

$$\ge -\mathsf{p}^* \underbrace{\left( \sum_{(t_1,\ldots,t_{j-1}) \in B} \prod_{1 \le i \le j-1} |\mathsf{p}_{E_i}(t_{i-1}, t_i) - \mathsf{p}^*| \right)}_{S_1}$$
$$\times \underbrace{\left( \sum_{(t_j,\ldots,t_{n-1}) \in C} \prod_{j+1 \le i \le n} |\mathsf{p}_{E_i}(t_{i-1}, t_i) - \mathsf{p}^*| \right)}_{S_2}.$$

These sums $S_1$ and $S_2$ should be studied independently. For $S_1$, we have

$$S_1 = \sum_{\substack{t_1 \in (\mathcal{M})_q : \\ C_{k_1,1}}} |\mathsf{p}_{E_1}(t_0, t_1) - \mathsf{p}^*| \sum_{\substack{t_2 \in (\mathcal{M})_q : \\ C_{k_2,2}}} |\mathsf{p}_{E_2}(t_1, t_2) - \mathsf{p}^*| \ldots$$
$$\times \sum_{\substack{t_{j-1} \in (\mathcal{M})_q : \\ C_{k_{j-1},j-1}}} |\mathsf{p}_{E_{j-1}}(t_{j-2}, t_{j-1}) - \mathsf{p}^*|$$
$$\le \sum_{\substack{t_1 \in (\mathcal{M})_q : \\ C_{k_1,1}}} |\mathsf{p}_{E_1}(t_0, t_1) - \mathsf{p}^*| \ldots$$

$$\times \sum_{\substack{t_{j-2}\in(\mathcal{M})_q:\\ C_{k_{j-2},j-2}}} |\mathsf{p}_{E_{j-2}}(t_{j-3},t_{j-2}) - \mathsf{p}^*| \times \|\mathsf{p}_{E_{j-1},t_{j-2}} - \mathsf{p}^*\|$$

$$\leq \mathbf{Adv}^{\mathrm{ncpa}}_{E_{j-1}}(q) \sum_{\substack{t_1\in(\mathcal{M})_q:\\ C_{k_1,1}}} |\mathsf{p}_{E_1}(t_0,t_1) - \mathsf{p}^*| \dots \sum_{\substack{t_{j-2}\in(\mathcal{M})_q:\\ C_{k_{j-2},j-2}}} |\mathsf{p}_{E_{j-2}}(t_{j-3},t_{j-2}) - \mathsf{p}^*|$$

$$\vdots$$

$$\leq \prod_{2\leq i\leq j-1} \mathbf{Adv}^{\mathrm{ncpa}}_{E_i}(q) \sum_{\substack{t_1\in(\mathcal{M})_q:\\ C_{k_1,1}}} |\mathsf{p}_{E_1}(t_0,t_1) - \mathsf{p}^*|$$

$$\leq \prod_{2\leq i\leq j-1} \mathbf{Adv}^{\mathrm{ncpa}}_{E_i}(q) \times \|\mathsf{p}_{E_1,t_0} - \mathsf{p}^*\|$$

$$\leq \prod_{1\leq i\leq j-1} \mathbf{Adv}^{\mathrm{ncpa}}_{E_i}(q).$$

Similarly one has:

$$S_2 = \sum_{\substack{t_{n-1}\in(\mathcal{M})_q:\\ C_{k_n,n}}} |\mathsf{p}_{E_n}(t_{n-1},t_n) - \mathsf{p}^*| \dots \sum_{\substack{t_j\in(\mathcal{M})_q:\\ C_{k_{j+1},j+1}}} |\mathsf{p}_{E_{j+1}}(t_j,t_{j+1}) - \mathsf{p}^*|$$

$$\leq \sum_{\substack{t_{n-1}\in(\mathcal{M})_q:\\ C_{k_n,n}}} |\mathsf{p}_{E_n}(t_{n-1},t_n) - \mathsf{p}^*| \dots$$

$$\times \sum_{\substack{t_{j+1}\in(\mathcal{M})_q:\\ C_{k_{j+2},j+2}}} |\mathsf{p}_{E_{j+2}}(t_{j+1},t_{j+2}) - \mathsf{p}^*| \times \|\mathsf{p}_{E^{-1}_{j+1},t_{j+1}} - \mathsf{p}^*\|$$

$$\leq \mathbf{Adv}^{\mathrm{ncpa}}_{E^{-1}_{j+1}}(q)$$

$$\times \sum_{\substack{t_{n-1}\in(\mathcal{M})_q:\\ C_{k_n,n}}} |\mathsf{p}_{E_n}(t_{n-1},t_n) - \mathsf{p}^*| \dots \sum_{\substack{t_{j+1}\in(\mathcal{M})_q:\\ C_{k_{j+2},j+2}}} |\mathsf{p}_{E_{j+2}}(t_{j+1},t_{j+2}) - \mathsf{p}^*|$$

$$\vdots$$

$$\leq \prod_{j+1\leq i\leq n} \mathbf{Adv}^{\mathrm{ncpa}}_{E^{-1}_i}(q),$$

from which the result follows. □

We can now prove the extension of Theorem 1.

**Theorem 2.** *Let $E_1,\dots,E_n$ be $n$ block ciphers with the same message space $\mathcal{M}$. For any integer $q$, one has*

$$\mathbf{Adv}^{\mathrm{cca}}_{E_n\circ\cdots\circ E_1}(q) \leq 2^{n-1} \max_{1\leq i\leq n} \left( \prod_{1\leq j\leq i-1} \mathbf{Adv}^{\mathrm{ncpa}}_{E_j}(q) \times \prod_{i+1\leq j\leq n} \mathbf{Adv}^{\mathrm{ncpa}}_{E^{-1}_j}(q) \right).$$

*Proof.* Fix any $q$-tuples $x_0, x_n \in (\mathcal{M})_q$. Then

$$
\begin{aligned}
&\mathsf{p}_{E_n \circ \cdots \circ E_1}(x, y) \\
&= \mathsf{p}^* + \sum_{(x_1,\ldots,x_{n-1}) \in ((\mathcal{M})_q)^{n-1}} \left( \prod_{1 \le i \le n} (\mathsf{p}_{E_i}(x_{i-1}, x_i) - \mathsf{p}^*) \right) && \text{(Lemma 5)} \\
&= \mathsf{p}^* + \sum_{k \in \{0,1\}^n} \sum_{\substack{(x_1,\ldots,x_{n-1}) \in \\ A_k(x_0,x_n)}} \left( \prod_{1 \le i \le n} (\mathsf{p}_{E_i}(x_{i-1}, x_i) - \mathsf{p}^*) \right) \\
&\ge \mathsf{p}^* + \sum_{\substack{k \in \{0,1\}^n : \\ k_1 + \ldots + k_n \equiv 1 \bmod 2}} \sum_{\substack{(x_1,\ldots,x_{n-1}) \in \\ A_k(x_0,x_n)}} \left( \prod_{1 \le i \le n} (\mathsf{p}_{E_i}(x_{i-1}, x_i) - \mathsf{p}^*) \right) \\
&\ge \mathsf{p}^* - 2^{n-1} \mathsf{p}^* \max_{1 \le i \le n} \left( \prod_{1 \le j \le i-1} \mathbf{Adv}^{\mathrm{ncpa}}_{E_j}(q) \prod_{i+1 \le j \le n} \mathbf{Adv}^{\mathrm{ncpa}}_{E_j^{-1}}(q) \right). && \text{(Lemma 6)}
\end{aligned}
$$

The result follows by Lemma 2. □

*Remark 1.* The upper bound of Theorem 2 is not tight in general already for $n = 2$. Indeed it is not hard to verify that Theorem 1 yields a better bound (at least when $E_1$ and $E_2^{-1}$ have different levels of NCPA-security).

**Corollary 1.** *Let $E_1, \ldots, E_n$ be $n$ block ciphers with the same message space $\mathcal{M}$. Fix $q \ge 1$. For $i = 1, \ldots, n$, let $\varepsilon_i = \max\{\mathbf{Adv}^{\mathrm{ncpa}}_{E_i}(q), \mathbf{Adv}^{\mathrm{ncpa}}_{E_i^{-1}}(q)\}$. Then one has*

$$\mathbf{Adv}^{\mathrm{cca}}_{E_n \circ \cdots \circ E_1}(q) \le 2^{n-1} \max_{1 \le i \le n} \prod_{\substack{1 \le j \le n \\ j \ne i}} \varepsilon_i.$$

*Remark 2.* It is actually not hard to see that Corollary 1 also holds with $\varepsilon_1 = \mathbf{Adv}^{\mathrm{ncpa}}_{E_1}(q)$ and $\varepsilon_n = \mathbf{Adv}^{\mathrm{ncpa}}_{E_n^{-1}}$, i.e., $E_1$ and $E_n$ need only be secure in one direction. Only the "internal" components $E_2, \ldots, E_{n-1}$ are required to be secure in both directions.

In the case of self-composition, we obtain the following corollary.

**Corollary 2.** *Let $E$ be a block cipher and $q \ge 1$. Denote*

$$\varepsilon = \max\{\mathbf{Adv}^{\mathrm{ncpa}}_{E}(q), \mathbf{Adv}^{\mathrm{ncpa}}_{E^{-1}}(q)\}.$$

*Then, for any integer $n \ge 1$,*

$$\mathbf{Adv}^{\mathrm{cca}}_{E^n}(q) \le (2\varepsilon)^{n-1}.$$

*Remark 3.* The assumption required for Corollary 2, namely that both $E$ and $E^{-1}$ are $(q, \varepsilon)$-NCPA secure, might seem much stronger than simply assuming

that $E$ is $(q, \varepsilon)$-NCPA secure. However, the schemes used in block ciphers are often involutions or close to involutions (for example balanced Feistel schemes). Then one needs to determine only *one* of these upper bounds. We stress that there exists block cipher designs such that the NCPA-security of $E^{-1}$ is much worse than the NCPA-security of $E$, the prominent example being type-1 generalized Feistel schemes [ZMI89, MV00], which is the basis for example of CAST-256.

## 5 On the Tightness of the Bound

The 2W1S theorem was shown to be tight in [MPR07] (see Appendix A of the full version of [MPR07]). In this section, we generalize the proof of tightness of [MPR07] to show that the bound of Theorem 2 is tight up to some constant.

As in [MPR07], denote $G$ the family of all permutations of $\mathcal{M}$ such that 0 lies on a cycle of length 2 (i.e., $\forall g \in G, g(g(0)) = 0$). Seeing $G$ as a block cipher[3], it can be shown that $\mathbf{Adv}_G^{\mathrm{ncpa}}(q) \leq \frac{2q}{|\mathcal{M}|}$ and $\mathbf{Adv}_G^{\mathrm{cca}}(2) \geq 1 - \frac{2}{|\mathcal{M}|}$. Then let us define the block cipher $F$ such that:

- with probability $\epsilon$, $F$ is the identity function $\mathcal{I}$,
- with probability $1 - \epsilon$, $F$ is uniformly randomly chosen in $G$.

Fix any constants $\delta, \delta', \delta'' > 0$. Then

$$\mathbf{Adv}_F^{\mathrm{ncpa}}(q) = \varepsilon \mathbf{Adv}_{\mathcal{I}}^{\mathrm{ncpa}}(q) + (1-\varepsilon)\mathbf{Adv}_G^{\mathrm{ncpa}}(q) \leq \varepsilon + \frac{2q}{|\mathcal{M}|} \leq (1+\delta)\varepsilon, \quad (4)$$

where for the last inequality we assumed $|\mathcal{M}|$ sufficiently large.

Now consider the block cipher $F^n$ for a fixed integer $n \geq 2$. Consider the adaptive distinguisher $\mathcal{D}$ making two queries to its permutation oracle $P$, $P(0)$ and then $P(P(0))$, and outputs 1 *iff* $P(P(0)) = 0$. When interacting with a random permutation, $\mathcal{D}$ outputs 1 with probability exactly[4] $2/|\mathcal{M}|$, while when it is interacting with $F^n$, it outputs 1 (at least) whenever $n-1$ among the $n$ instances of $F$ are the identity function, which happens with probability $n(1-\varepsilon)\varepsilon^{n-1}$. Hence, for any $q \geq 2$, one has

$$\mathbf{Adv}_{F^n}^{\mathrm{cca}}(q) \geq n(1-\varepsilon)\varepsilon^{n-1} - \frac{2}{|\mathcal{M}|} \geq \frac{n}{(1+\delta')(1+\delta'')}\varepsilon^{n-1},$$

where for the last inequality we assumed $\varepsilon$ sufficiently small and $|\mathcal{M}|$ sufficiently large. Using (4), we finally obtain

$$\mathbf{Adv}_{F^n}^{\mathrm{cca}}(q) \geq \frac{n}{(1+\delta)^{n-1}(1+\delta')(1+\delta'')}(\mathbf{Adv}_F^{\mathrm{ncpa}})^{n-1}.$$

[3] Ignoring efficiency considerations, this simply means that one defines the set of keys as $\mathcal{K} = G$.

[4] This can be seen as follows: with probability $1/|\mathcal{M}|$, 0 is a fixed point of $P$, and with probability $(|\mathcal{M}|-1)/(\mathcal{M}|(|\mathcal{M}|-1))$, one has $P(0) = y$ and $P(y) = 0$ for some $y \neq 0$.

Since $\delta$, $\delta'$, and $\delta''$ can be made arbitrarily close to zero, this essentially shows that the best upper bound one can hope for in Corollary 2 is $n\varepsilon^{n-1}$. Closing the gap between the proven upper bound $2^{n-1}\varepsilon^{n-1}$ and $n\varepsilon^{n-1}$ remains as an interesting open problem.

## A Omitted Proofs

*Proof. (of Lemma 1).* Fix some NCPA-distinguisher $\mathcal{D}$. Since we consider deterministic distinguishers, $\mathcal{D}$ is completely characterized by its $q$-tuple of queries $x = (x_1 \ldots, x_q)$ and its decision function $\phi_{\mathcal{D}} : (\mathcal{M})_q \to \{0,1\}$, where $\phi_{\mathcal{D}}(y)$ is the output of $\mathcal{D}$ when receiving $y = (y_1, \ldots, y_q)$ as answers to its queries. By definition of the advantage,

$$\begin{aligned}
\mathbf{Adv}(\mathcal{D}) &= \Big| \sum_{y \in (\mathcal{M})_q : \phi_{\mathcal{D}}(y)=1} \Pr\left[K \leftarrow_{\$} \mathcal{K} : E_K(x) = y\right] \\
&\qquad - \sum_{y \in (\mathcal{M})_q : \phi_{\mathcal{D}}(y)=1} \Pr\left[P \leftarrow_{\$} \mathsf{Perm}(\mathcal{M}) : P(x) = y\right] \Big| \\
&= \Big| \sum_{y \in (\mathcal{M})_q : \phi_{\mathcal{D}}(y)=1} (\mathsf{p}_{E,x}(y) - \mathsf{p}^*) \Big| \\
&\leq \|\mathsf{p}_{E,x} - \mathsf{p}^*\|.
\end{aligned}$$

By maximizing over $x \in (\mathcal{M})_q$, we obtain

$$\mathbf{Adv}_E^{\mathrm{ncpa}}(q) \leq \max_{x \in (\mathcal{M})_q} \|\mathsf{p}_{E,x} - \mathsf{p}^*\|.$$

To prove the equality of the two quantities, consider the distinguisher which queries the $q$-tuple $x$ which maximizes $\|\mathsf{p}_{E,x} - \mathsf{p}^*\|$, and outputs 1 *iff* the answer $y$ satisfies $\mathsf{p}_E(x,y) \geq \mathsf{p}^*$. Then the advantage of this distinguisher is exactly $\|\mathsf{p}_{E,x} - \mathsf{p}^*\|$, which concludes the proof. □

*Proof. (of Lemma 2).* Fix some CCA-distinguisher $\mathcal{D}$. Let $\tau$ be the transcript of the interaction of $\mathcal{D}$ with its permutation oracle, i.e., the ordered $q$-tuple of queries and answers $(b_i, z_i, z_i')$ where $b_i$ is a bit indicating whether the $i$-th query is direct or inverse, $z_i$ is the value queried to the oracle and $z_i'$ the answer. From this transcript, we define the *directionless* transcript $\tau' = (x, y)$, with $x = (x_1, \ldots, x_q)$ and $y = (y_1, \ldots, y_q)$ as follows: if the $i$-th query was a direct query, we let $x_i = z_i$ and $y_i = z_i'$, and if it was an inverse query we let $x_i = z_i'$ and $y_i = z_i$. We say that a transcript $\tau$ is *attainable* if there exists a permutation $P \in \mathsf{Perm}(\mathcal{M})$ such that the interaction of $\mathcal{D}$ with $P$ produces $\tau$ (in other words, the probability to obtain $\tau$ when $\mathcal{D}$ interacts with a random permutation is non-zero). Since the distinguisher is deterministic, there is a one-to-one mapping between attainable transcripts and attainable directionless transcripts. Let $\mathcal{T}$ denote the set of attainable directionless transcripts. Note that the interaction

of $\mathcal{D}$ with some permutation $P \in \mathsf{Perm}(\mathcal{M})$ produces the directionless transcript $\tau' = (x, y)$ *iff* $P(x) = y$. Note also that

$$\sum_{(x,y)\in\mathcal{T}} \mathsf{p}_E(x,y) = \sum_{(x,y)\in\mathcal{T}} \mathsf{p}^* = 1.$$

The output of the distinguisher is a function of the transcript $\tau$, or equivalently of the directionless transcript $\tau'$. Let $\mathcal{T}_0$ (resp. $\mathcal{T}_1$) be the set of attainable directionless transcripts $\tau'$ such that $\mathcal{D}$ outputs 0 (resp. 1) when obtaining $\tau' = (x, y)$. Then, by definition of the advantage,

$$\begin{aligned}\mathbf{Adv}(\mathcal{D}) &= \Big| \sum_{(x,y)\in\mathcal{T}_1} \Pr\left[P \leftarrow_{\$} \mathsf{Perm}(\mathcal{M}) : P(x) = y\right] \\ &\qquad\qquad - \sum_{(x,y)\in\mathcal{T}_1} \Pr\left[K \leftarrow_{\$} \mathcal{K} : E_K(x) = y\right] \Big| \\ &= \Big| \sum_{(x,y)\in\mathcal{T}_1} \mathsf{p}^* - \mathsf{p}_E(x,y) \Big|\end{aligned}$$

Using the assumption of the lemma, we have

$$\sum_{(x,y)\in\mathcal{T}_1} (\mathsf{p}^* - \mathsf{p}_E(x,y)) \le \sum_{(x,y)\in\mathcal{T}_1} \varepsilon \mathsf{p}^* \le \varepsilon \sum_{(x,y)\in\mathcal{T}_1} \mathsf{p}^* \le \varepsilon,$$

and similarly

$$\begin{aligned}-\sum_{(x,y)\in\mathcal{T}_1} (\mathsf{p}^* - \mathsf{p}_E(x,y)) &= \sum_{(x,y)\in\mathcal{T}_0} (\mathsf{p}^* - \mathsf{p}_E(x,y)) \\ &\le \sum_{(x,y)\in\mathcal{T}_0} \varepsilon \mathsf{p}^* \le \varepsilon \sum_{(x,y)\in\mathcal{T}_0} \mathsf{p}^* \le \varepsilon,\end{aligned}$$

from which the result follows. □

## References

[ABCV98] Aiello, W., Bellare, M., Di Crescenzo, G., Venkatesan, R.: Security amplification by composition: the case of doubly-iterated, ideal ciphers. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 390–407. Springer, Heidelberg (1998)

[BR06] Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 409–426. Springer, Heidelberg (2006)

[CPS14] Cogliati, B., Patarin, J., Seurin, Y.: Security amplification for the composition of block ciphers: simpler proofs and new results. Full version of this paper. Available from the authors of at http://eprint.iacr.org/

[GM09] Gaži, P., Maurer, U.: Cascade encryption revisited. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 37–51. Springer, Heidelberg (2009)

[HR10] Hoang, V.T., Rogaway, P.: On generalized Feistel networks. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 613–630. Springer, Heidelberg (2010)

[JÖS12] Jetchev, D., Özen, O., Stam, M.: Understanding adaptivity: random systems revisited. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 313–330. Springer, Heidelberg (2012)

[KNR09] Kaplan, E., Naor, M., Reingold, O.: Derandomized constructions of $k$-wise (almost) independent permutations. Algorithmica **55**(1), 113–133 (2009)

[Lee13] Lee, J.: Towards key-length extension with optimal security: cascade encryption and xor-cascade encryption. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 405–425. Springer, Heidelberg (2013)

[LPS12] Lampe, R., Patarin, J., Seurin, Y.: An asymptotically tight security analysis of the iterated even-mansour cipher. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 278–295. Springer, Heidelberg (2012)

[LR86] Luby, M., Rackoff, C.: Pseudo-random permutation generators and cryptographic composition. In: Symposium on Theory of Computing - STOC '86, pp. 356–363. ACM (1986)

[LS14] Lampe, R., Seurin, Y.: Security analysis of key-alternating Feistel ciphers. In: Fast Software Encryption - FSE 2014 (2014, to appear)

[Mau02] Maurer, U.M.: Indistinguishability of random systems. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 110–132. Springer, Heidelberg (2002)

[MP04] Maurer, U.M., Pietrzak, K.: Composition of random systems: when two weak make one strong. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 410–427. Springer, Heidelberg (2004)

[MPR07] Maurer, U.M., Pietrzak, K., Renner, R.S.: Indistinguishability amplification. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 130–149. Springer, Heidelberg (2007). Full version available at http://eprint.iacr.org/2006/456

[MRS09] Morris, B., Rogaway, P., Stegers, T.: How to encipher messages on a small domain. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 286–302. Springer, Heidelberg (2009)

[MT09] Maurer, U., Tessaro, S.: Computational indistinguishability amplification: tight product theorems for system composition. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 355–373. Springer, Heidelberg (2009)

[MV00] Moriai, S., Vaudenay, S.: On the pseudorandomness of top-level schemes of block ciphers. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 289–302. Springer, Heidelberg (2000)

[Mye04] Myers, S.: Black-box composition does not imply adaptive security. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 189–206. Springer, Heidelberg (2004)

[Pat90] Patarin, J.: Pseudorandom permutations based on the D.E.S. scheme. In: Cohen, G., Charpin, P. (eds.) EUROCODE 1990. LNCS, vol. 514, pp. 193–204. Springer, Heidelberg (1991)

[Pat91] Patarin, J.: New results on pseudorandom permutation generators based on the DES scheme. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 301–312. Springer, Heidelberg (1992)

[Pat08] Patarin, J.: The "coefficients H" technique. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 328–345. Springer, Heidelberg (2009)

[Pie05a] Pietrzak, K.: Composition does not imply adaptive security. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 55–65. Springer, Heidelberg (2005)

[Pie05b] Pietrzak, K.: Indistinguishability and composition of random systems. Ph.D. thesis, ETH Zurich, Switzerland (2005)

[Pie06] Pietrzak, K.: Composition implies adaptive security in minicrypt. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 328–338. Springer, Heidelberg (2006)

[Vau98] Vaudenay, S.: Provable security for block ciphers by decorrelation. In: Morvan, M., Meinel, C., Krob, D. (eds.) STACS 1998. LNCS, vol. 1373, pp. 249–275. Springer, Heidelberg (1998)

[Vau99] Vaudenay, S.: Adaptive-attack norm for decorrelation and super-pseudorandomness. In: Heys, H.M., Adams, C.M. (eds.) SAC 1999. LNCS, vol. 1758, pp. 49–61. Springer, Heidelberg (2000)

[Vau03] Vaudenay, S.: Decorrelation: a theory for block cipher security. J. Cryptol. **16**(4), 249–286 (2003)

[ZMI89] Zheng, Y., Matsumoto, T., Imai, H.: On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 461–480. Springer, Heidelberg (1990)