Towards Understanding the Known-Key Security of Block Ciphers

Elena Andreeva[1], Andrey Bogdanov[2] and Bart Mennink[1]

[1] Dept. Electrical Engineering, ESAT/COSIC, KU Leuven, and iMinds, Belgium
{elena.andreeva, bart.mennink}@esat.kuleuven.be
[2] Technical University of Denmark
anbog@dtu.dk

Abstract. Known-key distinguishers for block ciphers were proposed by Knudsen and Rijmen at ASIACRYPT 2007 and have been a major research topic in cryptanalysis since then. A formalization of known-key attacks in general is known to be difficult. In this paper, we tackle this problem for the case of block ciphers based on ideal components such as random permutations and random functions as well as propose new generic known-key attacks on generalized Feistel ciphers. We introduce the notion of known-key indifferentiability to capture the security of such block ciphers under a known key. To show its meaningfulness, we prove that the known-key attacks on block ciphers with ideal primitives to date violate security under known-key indifferentiability. On the other hand, to demonstrate its constructiveness, we prove the balanced Feistel cipher with random functions and the multiple Even-Mansour cipher with random permutations known-key indifferentiable for a sufficient number of rounds. We note that known-key indifferentiability is more quickly and tightly attained by multiple Even-Mansour which puts it forward as a construction provably secure against known-key attacks.
Keywords. Block ciphers, known-key security, known-key distinguishers, indifferentiability.

1 Introduction

Known-key attacks and our approach. *Known-key distinguishers* for block ciphers were introduced by Lars Knudsen and Vincent Rijmen at ASIACRYPT 2007 [25]. In the classical single secret-key setting, the attacker does not know the randomly generated key and aims to recover it or build another distinguisher for the cipher. The security model in known-key attacks is quite different though: the attacker knows the randomly drawn key the block cipher operates with and aims to find a structural property for the cipher under the known key – a property which an ideal cipher (a permutation drawn at random) would not have. An example of such a structural property from [25] is as follows. For an n-bit block cipher with a known key, the goal is to find a plaintext/ciphertext pair with the least $s < n/2$ significant bits zero. For the ideal cipher, the adversary needs to invest about 2^s encryptions. A cipher that allows one to find such a pair with

much less effort than 2^s encryptions is considered insecure in the known-key model. The seminal work [25] proposes a distinguisher for a permutation-based 7-round Feistel cipher and for 7 rounds of AES.

Since their introduction, known-key attacks have been a major research topic in the symmetric-key community. In explicit terms, there has been a great deal of effort towards refining and extending the distinguishers proposed by Knudsen and Rijmen, including generalizations to Rijndael [34, 44], SP-based Feistel ciphers [45–47] and some other constructions [17,35,37]. More importantly though, implicitly, known-key attacks have drawn attention to the security of block ciphers in the *open key model* where the adversary knows or even chooses keys. We think it is to some extent this renewed attention that eventually has given rise to a recent line of cryptanalytic results for the full AES: chosen-key distinguishers [7], related-key attacks [5–7] and single-key biclique meet-in-the-middle attacks [8] — all essentially exploiting the weaknesses of AES in the open key model.

Despite this cumulative impact in the symmetric-key community over the last years, known-key attacks have been known to be difficult to formalize since, formally speaking, it is not clear what an exploitable structural property of a block cipher under a known key is. There have been several attempts to solve the problem in general but we are not aware of any published results here. In this work, we take a slightly different approach to the problem: we focus on known-key distinguishers for *block ciphers based on idealized primitives* such as randomly drawn functions or permutations (examples of such constructions are balanced Feistel ciphers, generalized Feistel ciphers, and (multiple) Even-Mansour ciphers). For such block ciphers, we formulate the new notion of *known-key indifferentiability* which we believe captures the known-key security. To demonstrate its meaningfulness, we prove that the existing known-key attacks on block ciphers with idealized primitives actually lead to the violation of this notion. To demonstrate its constructiveness, we prove Feistel and Even-Mansour known-key indifferentiable for a sufficient number of rounds.

Indifferentiability framework. Traditionally, block ciphers have been examined under the classical notion of indistinguishability. In that setting a block cipher $\mathcal{C}$ is claimed secure if it is (computationally) indistinguishable from a fixed random permutation $\mathcal{R}$ with the same domain and range as $\mathcal{C}$. In other words, an attacker has to distinguish between $\mathcal{C}$ and $\mathcal{R}$ when placed in either *real* or *ideal* worlds, respectively. The seminal paper [27] of Luby and Rackoff showed that three (four) rounds of the Feistel construction, with independent pseudorandom functions in each round, yield a pseudorandom permutation (strong pseudorandom permutation) where the distinguisher does not have access to the internal functions. This result was followed by a number of works [21, 30, 36, 38–41, 52]. On the other hand, the indistinguishability of Even-Mansour cipher was only analyzed by [9, 18, 51]. Indistinguishability has been established as the *de facto* security notion for block ciphers because in the encryption setting the intended

use of the cipher key is in a secret manner; a fact comfortably accommodated by the notion of indistinguishability.

However, block ciphers find numerous and important uses beyond encryption. Block ciphers have been used as a building block for hash functions [19, 23, 26, 31, 33, 42, 50].[3] Here, the block cipher should work towards achieving the desired property of the higher level structure, and the cipher key is not necessarily secret, but known or easy to manipulate by a distinguisher. Clearly, indistinguishability cannot provide strong security guarantees in the open key model: a distinguisher's task becomes trivial once the key is known or chosen. Even more, if for example we decide to examine the indistinguishability "security" of a block cipher built out of an ideal underlying primitive (by explicitly giving to the distinguisher additional access to the internal primitive) in the open key setting, then again the notion indistinguishability falls short. A straightforward distinguishability attack here is possible in only two queries: one (K, M) query to the cipher $\mathcal{C}$ to obtain Y and one message and/or public key dependant x input to the underlying primitive $\mathcal{P}$ to help him compute Y' as a function of $\mathcal{C}_K$. The distinguisher needs to only verify if Y equals Y', which is true for the real construction $\mathcal{C}$ and false with high probability for a random permutation $\mathcal{R}$. The weakness of such an indistinguishability notion that allows access to the internal primitives lays in the fact that there is an obvious "constructive" gap in the ideal world where no communication between $\mathcal{R}$ and $\mathcal{P}$ is provided (as opposed to the real world where $\mathcal{C}$ evaluates on $\mathcal{P}$).

It is here where the notion of *indifferentiability* of Maurer et al. [29] comes into use to allow for: (i) arguing security in the open key model and (ii) enabling the distinguisher to gain access to the input/output behavior of the underlying primitive. The notion of indifferentiability argues the security of an idealized system built upon ideal underlying components, such as random functions or permutations. Initially, indifferentiability was used to analyze hash functions [1–4, 11, 20], more recently results for block ciphers have also appeared. In [15], Dodis and Puniya proved that the Feistel construction with a super-logarithmic number of rounds (random functions) is *indifferentiable* from an ideal permutation in the *honest-but-curious indifferentiability* model, where the adversary can only query the global Feistel construction and get all the intermediate results. The work of Coron et al. [10] attempted an indifferentiability proof for the Feistel construction with 6 rounds to obtain a fixed random permutation. But it were Holenstein et al. [22] who succeeded in proving a 14 round Feistel construction indifferentiable from a fixed random permutation. Weaker variants of the indifferentiability notion have appeared also in [16, 28, 53].

In its essence, indifferentiability, similarly to indistinguishability, aims at estimating the adversarial distinguishing advantage between the cipher $\mathcal{C}$ and $\mathcal{R}$ in the real and ideal worlds, respectively. Indifferentiability allows the adversary to access the underlying primitive(s) where the underlying ideal primitive(s) in the ideal world is replaced by a simulator $\mathcal{S}$, which aims to both mimic the behavior

[3] Many hash functions based on a fixed-key block cipher (also called permutation based hash functions) have also been proposed [32, 43, 48].

of the ideal primitive(s) and provide for responses that evaluate correctly when computed under the cipher composition. To fulfill the latter task the simulator is given access to the idealized system $\mathcal{R}$. That functionality of $\mathcal{S}$ allows for overcoming the existing "constructive" gap in the indistinguishability definition.

In fact, indifferentiability was introduced as the right notion to argue security of a block cipher as an ideal cipher, where each key names a new randomly chosen permutation. This theoretical treatment of block ciphers allows one to argue security results in a setting where the adversary freely chooses the key and each chosen key namely fixes a new random permutation. But while this interpretation might accommodate the analysis of block ciphers in the chosen key setting, it appears to be too strong for the case when the key is actually fixed but publicly known and thus the permutation is fixed. This brings us to our newly proposed notion of known-key indifferentiability (iff-KK), which examines the security of a block cipher as a composition from ideal primitives under a known key. Notice that an indifferentiability related view was already taken in the work of Mandal, Patarin and Seurin [28], who introduced the notion sequential indifferentiability and then relate it to that of correlation intractability in the ideal model to argue known key security. Our iff-KK notion is however more general and differs by the fact that it does not limit the adversary to make queries first to the underlying primitive and then to the cipher. Moreover, iff-KK explicitly provides the distinguisher with a public key which directly influences the queries to the block cipher and potentially the ones to the underlying primitives (whenever that is required by composition).

Our Contributions. The contributions of this paper are as follows:

Known-key attacks on type-I generalized Feistel networks. Knudsen-Rijmen [25] proposed known-key distinguishers on 7 rounds of the 2-line (balanced) Feistel network: $\mathrm{GFN}_{(2,7)}$ with any permutations and explicit key addition at the beginning of the round function. We propose a known-key attack on $4\ell - 1$ rounds of an ℓ-line permutation-based type-I generalized Feistel network: $\mathrm{GFN}_{(\ell,4\ell-1)}$ also with explicit key addition at the beginning of the round function. See Sect. 3.

Known-key indifferentiability. We propose a way to formalize the known-key security of block ciphers based on ideal primitives via the indifferentiability framework and put forward the notion of *known-key indifferentiability* in Sect. 4. By no means we claim to have formalized what a known-key attack is for all block ciphers and all existing attacks, but we do believe to have found an appropriate notion when the underlying components of the cipher are ideal (e.g. random permutations or random functions).

Meaningfulness of known-key indifferentiability. To show that our notion of known-key indifferentiability is useful and meaningful, we prove that the known-key attacks proposed to date on block ciphers with ideal components and explicit key input (namely, the attack by Knudsen-Rijmen on 7-round Feistel with

permutations, our attack on $(4\ell-1)$-round ℓ-line type-I Generalized Feistel construction, and an attack by Coron et al. and Mandal et al. [10, 28]) imply the known-key differentiability bound computed in Sect. 5.

Constructiveness of known-key indifferentiability. To demonstrate the constructiveness of our known-key indifferentiability notion, we prove two popular generic block cipher constructions known-key indifferentiable in Sect. 6. First, regarding the general indifferentiability result of [22], we prove that 14 rounds of balanced Feistel with random functions are known-key indifferentiable with a security bounds of $O(q^{16}/2^{n/2})$. Second, we prove that the multiple Even-Mansour construction instantiated with random permutations is perfectly known-key indifferentiable for any number of rounds starting from 1. As opposed to Feistel ciphers, this puts forward the Even-Mansour construction as particularly suitable for building known-key resistant ciphers.

2 Block Cipher Constructions

In this work, we mainly focus on known-key security of generalized Feistel networks and multiple Even-Mansour constructions.

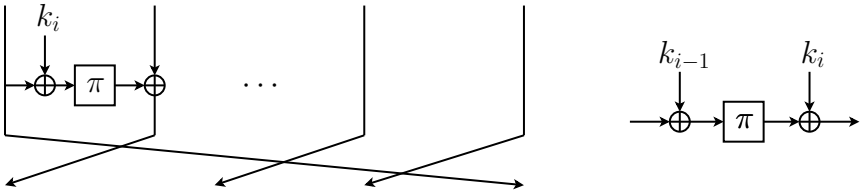

Fig. 1: For $1 \leq i \leq r$, round i of $\mathrm{GFN}_{(\ell,r)}$ with ℓ input lines (left) and EM_r (right, with XOR of previous key additionally included).

2.1 Generalized Feistel Networks

Feistel networks are very common block cipher designs, dating back to the design of Lucifer [49], and many generalizations of this design appeared in literature. In our work, we focus on type-I networks, as described by Zheng, Matsumoto and Imai [54], simply referring to it as generalized Feistel networks.

The generalized Feistel network $\mathrm{GFN}_{(\ell,r)} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ consists of r evaluations of a fixed random permutation π on n/ℓ bits, and it uses ℓ lines. For $i \in \{1,\ldots,r\}$, the i-th round ψ_i of $\mathrm{GFN}_{(\ell,r)}$ is defined as

$$\psi_i(p_1,\ldots,p_\ell) = (p_2 \oplus \pi(p_1 \oplus k_i), p_3, \ldots, p_\ell, p_1)\,,$$

where $k_1,\ldots,k_r$ denote the round keys derived from the master key K using some key schedule. The function ψ_i is depicted in Fig. 1. In this work, we also

consider a slightly modified variant of $\mathrm{GFN}_{(\ell,r)}$, where no keys are XORed with the inputs to the primitive, but instead, r *different* random functions $f_1, \ldots, f_r$ are employed. We refer to this construction as $\mathrm{GFNR}_{(\ell,r)}$, where the i-th round is defined as $\psi_i(p_1, \ldots, p_\ell) = (p_2 \oplus f_i(p_i), p_3, \ldots, p_\ell, p_1)$. Note that by construction, $\mathrm{GFNR}_{(\ell,r)}$ does not have an explicit key input. However, one can append an n-bit subkey to the input of function f_i if explicit key input is needed. In this case, random function f_i maps $(1 + 1/\ell)n$ bits to n/ℓ bits.

Luby and Rackoff showed in the setting where independent pseudorandom functions are used, three (four) rounds of the balanced Feistel construction (that is, $\mathrm{GFNR}_{(2,3)}$ and $\mathrm{GFNR}_{(2,4)}$) yield a pseudorandom permutation (strong pseudorandom permutation) where the distinguisher does not have access to the internal functions. This research line was followed up by a number of works [21, 30, 36, 38–41, 52].

2.2 Multiple Even-Mansour

The multiple Even-Mansour construction relates to the notion of key-alternating ciphers, which itself goes back to Daemen [12–14] and was used in the design of AES. However, it was Knudsen [24] who proposed to instantiate multiple-round key-alternating ciphers with randomly drawn, fixed and public permutations. The single-round key-alternating construction or EM_1 was proposed by Even-Mansour [18].

Multiple Even-Mansour constructions $\mathrm{EM}_r : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ consist of r evaluations of a fixed permutation π on n bits, which are separated by key addition. In other words,

$$\mathrm{EM}_r(K, p) = k_r \oplus \pi(\cdots \pi(k_1 \oplus \pi(k_0 \oplus p)) \cdots),$$

where $k_0, \ldots, k_r$ denote the round keys derived from the master key K using some key schedule. For $i \in \{1, \ldots, r\}$, round i of EM_r (together with the addition of the previous key) is depicted in Fig. 1.

In the setting where the r permutations are distinct and the round keys are independently generated and secret, Bogdanov et al. [9] recently proved that EM_r is indistinguishable from a randomly drawn permutation with less than $2^{2n/3}$ queries for $r \geq 2$, and Steinberger [51] improved this result to indistinguishability up to $2^{3n/4}$ queries for $r \geq 3$.

3 Known-Key Attacks on $\mathrm{GFN}_{(\ell,r)}$

Consider $\mathrm{GFN}_{(\ell,4\ell-1)}$ based on $r = 4\ell - 1$ calls to a random invertible function π. Label the incoming lines as $p = (p_1, \ldots, p_\ell)$ and the outgoing ones as $c = (c_1, \ldots, c_\ell)$. Denote by K the random, but known, master key, and let $k_1, \ldots, k_r$ be the r round keys. Denote the inputs to the i-th π-evaluations by $s_i \oplus k_i$. Note that there is a one-to-one correspondence between p and $(s_1, \ldots, s_\ell)$, as well as between c and $(s_{r-\ell+1}, \ldots, s_r)$. Following the idea of Knudsen and Rijmen [25],

the goal is to find tuples p, p' with corresponding c, c' that satisfy $p_1 \oplus c_2 = p'_1 \oplus c'_2$. Note that $c_2 = s_{r-\ell+2}$ by construction, and in our analysis we refrain from computing $(s_{r-\ell+3}, \ldots, s_r)$ if not needed.

Before describing the inputs p, p' chosen by the attacker, we first explain the attack. Let x be an arbitrary value, and consider $z, \alpha, \beta, \gamma, \delta$ variables to be determined later. Distinguisher D aims at the following intermediate state values

$$\begin{aligned}
s_{\ell+1} &= x \oplus k_{\ell+1} & s'_{\ell+1} &= x \oplus \alpha \oplus k_{\ell+1} \\
s_{\ell+2} &= x \oplus k_{\ell+2} & s'_{\ell+2} &= x \oplus \beta \oplus k_{\ell+2} \\
s_{\ell+3} &= x \oplus k_{\ell+3} & s'_{\ell+3} &= x \oplus k_{\ell+3} \\
&\vdots & &\vdots \\
s_{2\ell-1} &= x \oplus k_{2\ell-1} & s'_{2\ell-1} &= x \oplus k_{2\ell-1} \\
s_{2\ell} &= z \oplus k_{2\ell} & s'_{2\ell} &= z \oplus \gamma \oplus k_{2\ell} \\
s_{2\ell+1} &= x \oplus \delta \oplus k_{2\ell+1} & s'_{2\ell+1} &= x \oplus k_{2\ell+1}\,.
\end{aligned}$$

Here, we point out two exceptions from this general (otherwise) description of the attack. Firstly, for $\ell = 2$, s_4 and s'_4 adapt the value of $s_{2\ell}$ and $s'_{2\ell}$, and similarly for s_5 and s'_5. Secondly, for $\ell = 3$, s_6 and s'_6 follow the notation of $s_{2\ell}$ and $s'_{2\ell}$, and similarly for later state values. For $\ell > 3$ the description is non-ambiguous. Then, $s_\ell, \ldots, s_1$ and $s_{2\ell+2}, \ldots, s_r$ are computed in the straightforward way (i.e. using $s_i = s_{i+\ell} \oplus f(s_{i+\ell-1} \oplus k_{i+\ell-1})$), and similar for the s'-values. For $\ell > 3$, the general attack is depicted in Fig. 2. By construction, z and γ need to be such that $\pi(z) = \delta \oplus k_{\ell+1} \oplus k_{2\ell+1}$ (from $s_{\ell+1}$, $s_{2\ell}$, and $s_{2\ell+1}$) and $\pi(z \oplus \gamma) = \alpha \oplus k_{\ell+1} \oplus k_{2\ell+1}$ (from $s'_{\ell+1}$, $s'_{2\ell}$, and $s'_{2\ell+1}$). For the rest of the attack, we distinguish among $\ell = 2$, $\ell = 3$, and $\ell > 3$.

$\ell = 2$. Starting with $\ell = 2$ (this is in fact the attack of Knudsen and Rijmen [25]). Note that β does not occur in the analysis. We simply set $\gamma = 0$, and thus $\delta = \alpha$ and we require $\pi(z) = \alpha \oplus k_3 \oplus k_5$. It remains to determine the value α. We have:

$$\begin{aligned}
p_1 &= s_1 = x \oplus k_3 \oplus \pi(z \oplus k_2 \oplus k_4 \oplus \pi(x)) \\
c_2 &= s_7 = x \oplus \alpha \oplus k_5 \oplus \pi(z \oplus k_4 \oplus k_6 \oplus \pi(x \oplus \alpha)) \\
p'_1 &= s'_1 = x \oplus \alpha \oplus k_3 \oplus \pi(z \oplus k_2 \oplus k_4 \oplus \pi(x \oplus \alpha)) \\
c'_2 &= s'_7 = x \oplus k_5 \oplus \pi(z \oplus k_4 \oplus k_6 \oplus \pi(x))\,.
\end{aligned}$$

As demonstrated in [25], $p_1 \oplus c_2 = p'_1 \oplus c'_2$ holds if $\alpha = x \oplus \pi^{-1}(\pi(x) \oplus k_2 \oplus k_6)$. The tuples p and p' queried by D are easily derivable and not discussed.

$\ell = 3$. Next we consider $\ell = 3$. This case turns out to require a special treatment. We have:

$$\begin{aligned}
p_1 &= s_1 = x \oplus k_4 \oplus \pi(z \oplus k_3 \oplus k_6 \oplus \pi(x)) \\
c_2 &= s_{10} = x \oplus \delta \oplus k_7 \oplus \pi(z \oplus k_6 \oplus k_9 \oplus \pi(x \oplus k_5 \oplus k_8 \oplus \pi(x \oplus \delta))) \\
p'_1 &= s'_1 = x \oplus \alpha \oplus k_4 \oplus \pi(z \oplus \gamma \oplus k_3 \oplus k_6 \oplus \pi(x \oplus \beta)) \\
c'_2 &= s'_{10} = x \oplus k_7 \oplus \pi(z \oplus \gamma \oplus k_6 \oplus k_9 \oplus \pi(x \oplus \beta \oplus k_5 \oplus k_8 \oplus \pi(x)))\,.
\end{aligned}$$

Note that

$$\begin{aligned} p_1 \oplus c_2 &= \pi(z) \oplus \pi(z \oplus k_3 \oplus k_6 \oplus \pi(x)) \oplus \\ &\qquad \pi(z \oplus k_6 \oplus k_9 \oplus \pi(x \oplus k_5 \oplus k_8 \oplus \pi(x \oplus \delta))) \\ p'_1 \oplus c'_2 &= \pi(z \oplus \gamma) \oplus \pi(z \oplus \gamma \oplus k_3 \oplus k_6 \oplus \pi(x \oplus \beta)) \oplus \\ &\qquad \pi(z \oplus \gamma \oplus k_6 \oplus k_9 \oplus \pi(x \oplus \beta \oplus k_5 \oplus k_8 \oplus \pi(x))) \,. \end{aligned}$$

Our goal is these values to satisfy $p_1 \oplus c_2 = p'_1 \oplus c'_2$, but the same approach as for $\ell = 2$ (and [25]) does not work here. However, if we take δ such that $\pi(x \oplus k_5 \oplus k_8 \oplus \pi(x \oplus \delta)) = k_6 \oplus k_9$, and β such that $\pi(x \oplus \beta \oplus k_5 \oplus k_8 \oplus \pi(x)) = k_6 \oplus k_9$, and $\gamma = \pi(x) \oplus \pi(x \oplus \beta)$, the desired equation is satisfied. Then, by construction, $z = \pi^{-1}(\delta \oplus k_4 \oplus k_7)$ and $\alpha = \pi(z \oplus \gamma) \oplus k_4 \oplus k_7$. The tuples p and p' queried by D are easily derivable and not discussed.

$\ell > 3$. Remains to consider the general case, $\ell > 3$. This attack is visualized in Fig. 2. In this case, we simply set $\gamma = 0$, and thus $\delta = \alpha$ and we require $\pi(z) = \alpha \oplus k_{\ell+1} \oplus k_{2\ell+1}$. It remains to determine the values α and β. We find:

$$\begin{aligned} p_1 = s_1 &= x \oplus k_{\ell+1} \oplus \pi(z \oplus k_\ell \oplus k_{2\ell} \oplus \pi(x)) \\ c_2 = s_{3\ell+1} &= x \oplus \alpha \oplus k_{2\ell+1} \oplus \pi(z \oplus k_{2\ell} \oplus k_{3\ell} \oplus \tilde{\pi}(K, x, \alpha)) \\ p'_1 = s'_1 &= x \oplus \alpha \oplus k_{\ell+1} \oplus \pi(z \oplus k_\ell \oplus k_{2\ell} \oplus \pi(x)) \\ c'_2 = s'_{3\ell+1} &= x \oplus k_{2\ell+1} \oplus \pi(z \oplus k_{2\ell} \oplus k_{3\ell} \oplus \tilde{\pi}'(K, x, \alpha, \beta)) \,, \end{aligned}$$

where

$$\begin{aligned} \tilde{\pi}(K, x, \alpha) &= \pi(x \oplus k_{2\ell-1} \oplus k_{3\ell-1} \oplus \cdots \pi(x \oplus k_{\ell+2} \oplus k_{2\ell+2} \oplus \\ &\qquad \pi(x \oplus k_{\ell+1} \oplus k_{2\ell+1} \oplus \pi(x \oplus \alpha))) \cdots) \\ \tilde{\pi}'(K, x, \alpha, \beta) &= \pi(x \oplus k_{2\ell-1} \oplus k_{3\ell-1} \oplus \cdots \pi(x \oplus \beta \oplus k_{\ell+2} \oplus k_{2\ell+2} \oplus \\ &\qquad \pi(x \oplus \alpha \oplus k_{\ell+1} \oplus k_{2\ell+1} \oplus \pi(x))) \cdots) \,. \end{aligned}$$

Note that

$$\begin{aligned} p_1 \oplus c_2 \oplus p'_1 \oplus c'_2 &= \pi(z \oplus k_{2\ell} \oplus k_{3\ell} \oplus \tilde{\pi}(K, x, \alpha)) \oplus \\ &\qquad \pi(z \oplus k_{2\ell} \oplus k_{3\ell} \oplus \tilde{\pi}'(K, x, \alpha, \beta)) \,. \end{aligned}$$

We now put α to satisfy $\tilde{\pi}(K, x, \alpha) = k_{2\ell} \oplus k_{3\ell}$ (note that by the construction of $\tilde{\pi}$ this is really possible), and β to satisfy $\tilde{\pi}'(K, x, \alpha, \beta) = k_{2\ell} \oplus k_{3\ell}$ for this given α. This choice is well-defined: α is defined as a function of K and x, while β and z are a function of K, x, and α. The tuples p and p' queried by D are easily derivable and not discussed.

Conclusion of the attack. Once x is arbitrarily chosen, $z, \alpha, \beta, \gamma, \delta$ are easily computable from K and x. For $\mathrm{GFN}_{(\ell,4\ell-1)}$, the resulting plaintexts and ciphertexts satisfy $p_1 \oplus c_2 = p'_1 \oplus c'_2$ with probability 1. This equation is, however, satisfied by an ideal cipher $\mathcal{R}$ with probability at most $1/2^{n/\ell}$. This completes the attack.

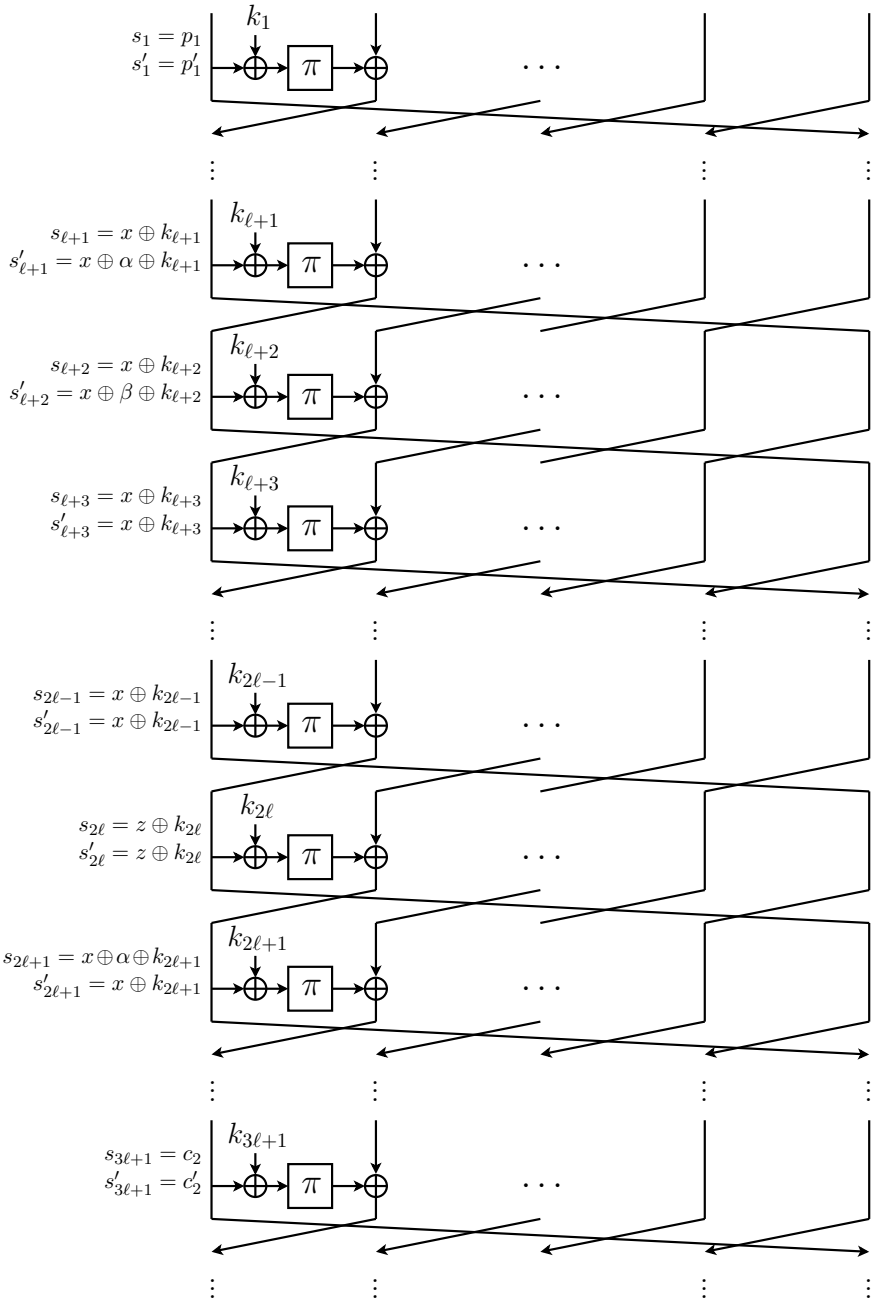

Fig. 2: Attack of Sect. 3 for $\ell > 3$. Parameter x can be freely chosen, parameters α ($= \beta$), γ, and z depend on x and the round keys, and are explained in the text.

4 Known-Key Indifferentiability for Block Ciphers

Consider a composed system $\mathcal{C} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ based on an underlying idealized primitive $\mathcal{P} : \{0,1\}^\kappa \times \{0,1\}^x \to \{0,1\}^y$. Here, $\mathcal{C}$ is always a keyed primitive (i.e., a block cipher), but $\mathcal{P}$ may or may not be keyed, and the key space may differ from that of $\mathcal{C}$. Furthermore, depending on $\mathcal{C}$, $\mathcal{P}$ denotes either a single or a composition of multiple idealized primitives $\mathcal{P}_i$.

Where the classical notion of indistinguishability is established to provide strong security guarantees in the *secret* key setting, this is not true in the *open* key model where chosen or known keys come into play. In the latter setting, one can benefit from the known indifferentiability definition introduced in the work of Maurer et al. [29] and adapted for the case of hash functions by Coron et al. [11]. Building upon these results, we propose a new definition of known-key security. Our definition differs from earlier weaker versions of indifferentiability [11, 16, 28, 53] by its generality and the fact that it explicitly provides the distinguishing adversary with a public key under which it queries both the block cipher and potentially the underlying primitives (if that is required by composition). It moreover, does not limit the adversary's type of queries, as is the case for leaky, public, and sequential indifferentiability.

We thus propose the following formalization:

Definition 1. *Let $\mathcal{C}$ be a composed primitive with oracle access to an ideal primitive $\mathcal{P}$. Let $\mathcal{R}$ be an ideal primitive with the same domain and range as $\mathcal{C}$. Let $\mathcal{S}$ be a simulator with the same domain and range as $\mathcal{P}$ with oracle access to $\mathcal{R}$ and making at most $q_{\mathcal{S}}$ queries, and let D be a distinguisher making at most q_{D} queries. The known-key indifferentiability advantage $\mathbf{Adv}^{\text{iff-KK}}_{\mathcal{C},\mathcal{S}}(\mathsf{D})$ of D is defined as*

$$\left|\Pr\left(K \xleftarrow{\$} \{0,1\}^k; \mathsf{D}^{\mathcal{C}^{\mathcal{P}},\mathcal{P}}(K) = 1\right) - \Pr\left(K \xleftarrow{\$} \{0,1\}^k; \mathsf{D}^{\mathcal{R},\mathcal{S}^{\mathcal{R}}}(K) = 1\right)\right| .$$

By $\mathbf{Adv}^{\text{iff-KK}}_{\mathcal{C},\mathcal{S}}(q_{\mathsf{D}})$ we denote the maximum advantage of any distinguisher making at most q_{D} queries to its oracles. Primitive $\mathcal{C}$ is said to be $(q_{\mathsf{D}}; q_{\mathcal{S}}; \varepsilon)$ indifferentiable from $\mathcal{R}$ if $\mathbf{Adv}^{\text{iff-KK}}_{\mathcal{C},\mathcal{S}}(q_{\mathsf{D}}) < \varepsilon$.

In this indifferentiability experiment, the distinguisher is provided with access to either of two worlds: *left (real)* and *right (ideal)*. In the *left* world the distinguisher D has a query access to the composed construction $\mathcal{C}$ and the primitive $\mathcal{P}$, while in the *right* world D accesses the ideal primitive $\mathcal{R}$ and the simulator $\mathcal{S}$, respectively. In case the composed primitive $\mathcal{C}$ is invertible, D obtains access to it in both forward and backward (inverse) direction. We refer to $\mathcal{C}$ and $\mathcal{R}$ as the "composed" oracles $\mathcal{O}_1$, and these oracles always respond under the known-key K. Hence, D can forward query a message input M to receive $C = \mathcal{C}(K, M)$ in the left world and $C = \mathcal{R}(M)$ in the right world (here the randomly chosen key K implicitly fixes an instance of $\mathcal{R}$), or D can also backward query C to receive $M = \mathcal{C}^{-1}(K, C)$ and $M = \mathcal{R}^{-1}(M)$ in the left and right worlds, respectively. We refer to $\mathcal{P}$ and $\mathcal{S}$ as the "small" oracles $\mathcal{O}_2$, to which D has full access (i.e., even if $\mathcal{C}$ is designed to query $\mathcal{P}$ only on the key K), but we note that $\mathcal{S}$ knows

this public key K. From a practical point of view, the full access to the small oracles makes perfect sense, as the original idea of indifferentiability is that the distinguisher may know the underlying structure, and thus, use the underlying primitive as it wishes.

The particular way of allowing the key input to the composed primitive to be always the known key K but the key input to the small primitive to be anything, sets this known-key indifferentiability definition apart from existing versions of indifferentiability like [11, 16, 28, 53]. In more detail, in Table 1, we compare the interfaces in Def. 1 with the ones used in the indifferentiability definition (see [10, 22] for its block cipher instantiation). As it turns out, this change makes our definition particularly suitable for analyzing known-key security. In Prop. 1, we prove that iff implies iff-KK. Moreover, in Sect. 6 we also show a counterexample that an implication in the opposite direction does not hold.

Table 1: Interface of D with the composed oracle $\mathcal{O}_1$ ($\mathcal{C}$ in the left world, $\mathcal{R}$ in the right world) in the standard indifferentiability setting and in Def. 1. For both security definitions, the interface with the right oracle $\mathcal{O}_2$ is the same: D has full access to $\mathcal{O}_2$.

Indifferentiability	forward O_1 query	inverse O_1 query
Indifferentiability (iff)	$(K, M) \longrightarrow C = \mathcal{O}_1(K, M)$	$(K, C) \longrightarrow M = \mathcal{O}_1^{-1}(K, C)$
Known-key indiff. (iff-KK) ($K \xleftarrow{\$} \{0,1\}^k$ fixed, public)	$M \longrightarrow C = \mathcal{O}_1(K, M)$	$C \longrightarrow M = \mathcal{O}_1^{-1}(K, C)$

Proposition 1. *If $\mathcal{C}$ is $(q_{\mathsf{D}}; q_{\mathcal{S}}; \varepsilon)$* iff*-secure block cipher, then it is $(q_{\mathsf{D}}; q_{\mathcal{S}}; \varepsilon)$* iff-KK*-secure.*

Proof. Let $\mathcal{S}$ be a simulator such that for any distinguisher D making at most q_{D} queries, the iff advantage is at most ε. We define $\mathcal{S}' = \mathcal{S}$ to be the simulator for the iff-KK security. We prove that for any iff-KK distinguisher D' making at most q_{D} queries, we have $\mathbf{Adv}^{\text{iff-KK}}_{\mathcal{C},\mathcal{S}'}(\mathsf{D}') < \varepsilon$.

Let D' be any such distinguisher. We build an iff distinguisher D using D' that has the same advantage in breaking $\mathcal{C}$. Distinguisher D simulates the environment for D' as follows: firstly, it selects uniformly at random a key $K \xleftarrow{\$} \{0,1\}^k$ and runs D' on input K; then it forwards all queries by D' to its own oracles. If D' succeeds in distinguishing the left and right worlds, D succeeds as well. In particular, we have $\mathbf{Adv}^{\text{iff-KK}}_{\mathcal{C},\mathcal{S}'}(\mathsf{D}') = \mathbf{Adv}^{\text{iff}}_{\mathcal{C},\mathcal{S}}(\mathsf{D}) < \varepsilon$.

5 Known-Key Indifferentiability is Meaningful

Consider any known-key distinguishing attack on a block cipher $\mathcal{C}$ with idealized primitive $\mathcal{P}$. Let $K \in \{0,1\}^k$ be a known key. A classical known-key distinguisher

for a function $\mathcal{C}(K,\cdot)$ based on ideal primitive $\mathcal{P}$ operates as follows: it makes q queries to its primitives, and then it outputs 1 if the queries show some "unexpected" relation, which means that such relation should not hold for a random primitive $\mathcal{R}$ with the same domain and range of $\mathcal{C}$. We formalize and translate such known-key distinguisher D to a distinguisher for the indifferentiability notion iff-KK as follows. Let $\mathcal{S}$ be a simulator. In advance of making any queries, this distinguisher fixes a predicate $\varphi(\mathcal{Q})$, where $\mathcal{Q}$ is a list of query tuples. Then, the distinguisher makes q_{D} queries to its left and right oracles, to obtain a query history $\mathcal{Q}_{q_{\mathsf{D}}}$ of size q_{D}. If $\varphi(\mathcal{Q}_{q_{\mathsf{D}}})$ holds, it outputs 1, and otherwise it outputs 0. Clearly, D bases its decision solely on the predicate $\varphi(\mathcal{Q}_{q_{\mathsf{D}}})$, and by Def. 1:

$$\begin{aligned}\mathbf{Adv}^{\text{iff-KK}}_{\mathcal{C},\mathcal{S}}(q_{\mathsf{D}}) &\geq \mathbf{Adv}^{\text{iff-KK}}_{\mathcal{C},\mathcal{S}}(\mathsf{D}) \\ &= \left|\Pr\left(\varphi(\mathcal{Q}_{q_{\mathsf{D}}}) \text{ for } \mathcal{C}^{\mathcal{P}},\mathcal{P}\right) - \Pr\left(\varphi(\mathcal{Q}_{q_{\mathsf{D}}}) \text{ for } \mathcal{R},\mathcal{S}^{\mathcal{R}}\right)\right| .\end{aligned} \tag{1}$$

Now, in classical known-key distinguishing attacks, the first probability is (close to) 1, while the second probability is significantly smaller. Note that for the second probability, the distinguisher may ask queries to the simulator $\mathcal{S}$, but in order for $\mathcal{S}$ to be successful, it will try to consult $\mathcal{R}$ as often as possible and queries to $\mathcal{S}$ can consequently be seen as indirect queries to $\mathcal{R}$.

We demonstrate this approach using the attack of Sect. 3 on $\text{GFN}_{(\ell,4\ell-1)}$ and an attack on $\text{GFNR}_{(2,5)}$ by Coron et al. and Mandal et al. [10, 28], therewith demonstrating that this approach applies to *any* known-key distinguishing attack known in literature.

Theorem 1. *Let $\mathcal{C}$ be $GFN_{(\ell,r)} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ for $r = 4\ell - 1$ with oracle access to an ideal primitive $\mathcal{P} = \pi : \{0,1\}^{n/\ell} \to \{0,1\}^{n/\ell}$ (cf. Sect. 3). Let $\mathcal{R}$ denote an ideal cipher with the same domain and range as $\mathcal{C}$. For any simulator $\mathcal{S}$ that makes at most $q_{\mathcal{S}} \leq 2^{n-1} - 1$ queries to $\mathcal{R}$, there exists a distinguisher D that makes at most $2r + 2$ queries to its oracles, such that*

$$\mathbf{Adv}^{\text{iff-KK}}_{\mathcal{C},\mathcal{S}}(\mathsf{D}) \geq 1 - \frac{q_{\mathcal{S}}^2 + 2}{2^{n/\ell}} .$$

Proof. Let $\mathcal{S}$ be any simulator making at most $q_{\mathcal{S}}$ queries to $\mathcal{R}$. Let $K \xleftarrow{\$} \{0,1\}^k$ be the given key, and $k_1, \ldots, k_r$ be the round keys. We construct a distinguisher D that differentiates $(\mathcal{C},\mathcal{P})$ from $(\mathcal{R},\mathcal{S})$ with high probability. Define predicate $\varphi(\mathcal{Q})$ as follows:

$$\exists\, (p_1 \ldots p_\ell; c_1 \ldots c_\ell), (p'_1 \ldots p'_\ell; c'_1 \ldots c'_\ell) \in \mathcal{Q} \text{ such that } p_1 \oplus c_2 = p'_1 \oplus c'_2 . \tag{2}$$

The distinguisher makes $2r$ queries to $\mathcal{P}$ as explained in Sect. 3. Then, it makes its two corresponding queries to the left oracle, which results in $\mathcal{Q}_{2r+2}$ containing exactly two left oracle queries. By construction,

$$\Pr\left(\varphi(\mathcal{Q}_{2r+2}) \text{ for } \text{GFN}^{\mathcal{P}}_{(\ell,r)},\mathcal{P}\right) = 1 .$$

Remains to consider the probability $\varphi(\mathcal{Q}_{2r+2})$ holds in the other game. Suppose the simulator makes $q_{\mathcal{S}}$ queries, denote by $\mathcal{Q}^{\mathcal{S}}$ the query history of $\mathcal{S}$ to $\mathcal{R}$. By basic probability theory:

$$\begin{aligned}\Pr\left(\varphi(\mathcal{Q}_{2r+2}) \text{ for } \mathcal{R}, \mathcal{S}^{\mathcal{R}}\right) &= \Pr\left(\varphi(\mathcal{Q}_{2r+2}) \text{ for } \mathcal{R}, \mathcal{S}^{\mathcal{R}} \mid \varphi(\mathcal{Q}^{\mathcal{S}})\right) \Pr\left(\varphi(\mathcal{Q}^{\mathcal{S}})\right) + \\ &\quad \Pr\left(\varphi(\mathcal{Q}_{2r+2}) \text{ for } \mathcal{R}, \mathcal{S}^{\mathcal{R}} \mid \neg\varphi(\mathcal{Q}^{\mathcal{S}})\right) \Pr\left(\neg\varphi(\mathcal{Q}^{\mathcal{S}})\right) \\ &\leq \Pr\left(\varphi(\mathcal{Q}^{\mathcal{S}})\right) + \Pr\left(\varphi(\mathcal{Q}_{2r+2}) \text{ for } \mathcal{R}, \mathcal{S}^{\mathcal{R}} \mid \neg\varphi(\mathcal{Q}^{\mathcal{S}})\right).\end{aligned}$$

We first consider $\Pr\left(\varphi(\mathcal{Q}^{\mathcal{S}})\right)$. Any two queries the simulator makes to $\mathcal{R}$ satisfy $p_1 \oplus c_2 = p_1' \oplus c_2'$ with probability at most $\frac{2^{n-n/\ell}}{2^n - q_{\mathcal{S}}}$, as any query is randomly drawn from a set of size at least $2^n - q_{\mathcal{S}}$. Consequently, as the simulator makes $q_{\mathcal{S}}$ queries, and any couple may result in a collision,

$$\Pr\left(\varphi(\mathcal{Q}^{\mathcal{S}})\right) \leq \binom{q_{\mathcal{S}}}{2} \frac{2^{n-n/\ell}}{2^n - q_{\mathcal{S}}}.$$

Regarding the second probability: conditioned on $\neg\varphi(\mathcal{Q}^{\mathcal{S}})$, (2) may still hold if the two queries the distinguisher makes to $\mathcal{R}$ accidentally satisfy it. As the second oracle query is drawn from a set of size at least $2^n - (q_{\mathcal{S}} + 1)$, the queries satisfy $p_1 \oplus c_2 = p_1' \oplus c_2'$ with probability at most $\frac{2^{n-n/\ell}}{2^n - (q_{\mathcal{S}}+1)}$. Concluding, we find

$$\Pr\left(\varphi(\mathcal{Q}_{2r+2}) \text{ for } \mathcal{R}, \mathcal{S}^{\mathcal{R}}\right) \leq \left(\binom{q_{\mathcal{S}}}{2} + 1\right) \frac{2^{n-n/\ell}}{2^n - (q_{\mathcal{S}} + 1)} \leq \frac{q_{\mathcal{S}}^2 + 2}{2^{n/\ell}},$$

where we use that $2^n - (q_{\mathcal{S}} + 1) \geq 2^{n-1}$ for $q_{\mathcal{S}} + 1 \leq 2^{n-1}$. Hence, we find $\mathbf{Adv}^{\text{iff-KK}}_{\mathcal{C},\mathcal{S}}(2r+2) \geq 1 - \frac{q_{\mathcal{S}}^2+2}{2^{n/\ell}}$. □

Next we consider a distinguishing attack described in [10] and [28, App. C].

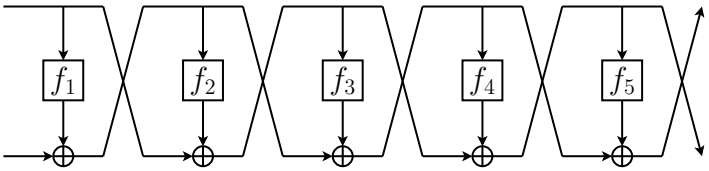

Fig. 3: $\text{GFNR}_{(2,5)}$ (see Thm. 2).

Theorem 2. *Let $\mathcal{C}$ be $GFNR_{(2,5)} : \{0,1\}^n \to \{0,1\}^n$ with oracle access to 5 ideal primitives $\mathcal{P} = (f_1, \ldots, f_5)$ with $f_i : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ (see Fig. 3). Let $\mathcal{R}$ denote an ideal permutation with the same domain and range as $\mathcal{C}$. For any simulator $\mathcal{S}$ that makes at most $q_{\mathcal{S}} \leq 2^{n-1} - 1$ queries to $\mathcal{R}$, there exists a distinguisher D that makes at most 24 queries to its oracles, such that*

$$\mathbf{Adv}^{\text{iff-KK}}_{\mathcal{C},\mathcal{S}}(\mathsf{D}) \geq 1 - \frac{q_{\mathcal{S}}^4 + 2}{2^{n/2}}.$$

Proof. Denote the inputs of a $\mathrm{GFNR}_{(2,5)}$ evaluation by (p, r) and the outputs by (c, d). The attack of [10] and [28, App. C] describes a way to find 4 plaintext-ciphertext pairs that satisfy $p_1 \oplus p_2 \oplus p_3 \oplus p_4 = d_1 \oplus d_2 \oplus d_3 \oplus d_4 = 0$. As in Thm. 1, predicate $\varphi(\mathcal{Q})$ is defined as follows:

$$\exists\, (p_1, r_1; c_1, d_1), \ldots, (p_4, r_4; c_4, d_4) \in \mathcal{Q} \text{ such that} \\ p_1 \oplus p_2 \oplus p_3 \oplus p_4 = d_1 \oplus d_2 \oplus d_3 \oplus d_4 = 0\,. \qquad (3)$$

The distinguisher makes 20 queries to $\mathcal{P}$ (as in the proof of Thm. 1), and the four corresponding queries to the left oracle, which results in $\mathcal{Q}_{24}$. By construction, $\varphi(\mathcal{Q}_{24})$ holds for $\mathrm{GFN}^{\mathcal{P}}_{(2,5)}, \mathcal{P}$ with probability 1, and it remains to consider the probability $\varphi(\mathcal{Q}_{24})$ holds in the other game. Similar to the proof of Thm. 1, we find

$$\Pr\left(\varphi(\mathcal{Q}_{24}) \text{ for } \mathcal{R}, \mathcal{S}^{\mathcal{R}}\right) \leq \binom{q_{\mathcal{S}}}{4} \frac{2^{n/2}}{2^n - q_{\mathcal{S}}} + \frac{2^{n/2}}{2^n - (q_{\mathcal{S}} + 1)}\,,$$

and hence we obtain $\mathbf{Adv}^{\text{iff-KK}}_{\mathcal{C},\mathcal{S}}(24) \geq 1 - \frac{q_{\mathcal{S}}^4 + 2}{2^{n/2}}$, for $q_{\mathcal{S}} + 1 \leq 2^{n-1}$. □

6 Known-Key Indifferentiability is Constructive

The next obvious question then is, whether there exist block cipher constructions that are known-key indifferentiable from an ideal cipher. In this section, we prove that this is indeed the case.

First, we consider generalized Feistel networks. In [22], Holenstein et al. considered $\mathrm{GFNR}_{(2,14)}$, a variant of $\mathrm{GFN}_{(2,14)}$ where the keys are not XORed to get the input to the primitives, but are used to obtain 14 different random functions (see also Sect. 2), and proved that this construction has indifferentiable advantage from an ideal cipher of $O(q^{16}/2^{n/2})$. Here, we refer to standard indifferentiability (see Table 1 for the interfaces in this notion). Using this result, we obtain the following theorem.

Theorem 3. *Let $\mathcal{C}$ be $GFNR_{(2,14)}$ with oracle access to an ideal primitive $\mathcal{P}$ consisting of 14 random functions (and where no round keys are XORed). Let D be an arbitrary distinguisher making at most q queries. Then there exists a simulator $\mathcal{S}$ such that*

$$\mathbf{Adv}^{\text{iff-KK}}_{\mathcal{C},\mathcal{S}}(\mathsf{D}) = O(q^{16}/2^{n/2})\,,$$

where $\mathcal{S}$ makes at most $1400q^8$ queries to $\mathcal{R}$ and runs in time $O(q^8)$.

Proof. Holenstein et al. [22] proved that for $\mathcal{C}$ being $\mathrm{GFN}_{(2,14)}$ any distinguisher making at most q queries, has indifferentiability an advantage of $\mathbf{Adv}^{\text{iff}}_{\mathcal{C},\mathcal{S}}(\mathsf{D}) = O(q^{16}/2^{n/2})$. Their simulator makes at most $1400q^8$ queries to $\mathcal{R}$ and runs in time $O(q^8)$. From Prop. 1, we conclude that the same bound holds for the iff-KK-security of $\mathrm{GFN}_{(2,14)}$, which completes the proof. □

Next, we consider multiple Even-Mansour, and show that already with one round, this construction turns out to be optimally known-key indifferentiable secure.

Theorem 4. *Let for $r \geq 1$, $\mathcal{C}_r$ be EM_r with oracle access to an ideal primitive $\mathcal{P}$ consisting of r random permutations. Let D be an arbitrary distinguisher making at most q queries. Then there exists a simulator $\mathcal{S}$ such that*

$$\mathbf{Adv}^{\text{iff-KK}}_{\mathcal{C},\mathcal{S}}(\mathsf{D}) = 0\,,$$

where $\mathcal{S}$ makes at most q queries to $\mathcal{R}$ and runs in time $O(q)$.

Proof. First, consider $r = 1$. Let $k_0 \| k_1 \xleftarrow{\$} \{0,1\}^{2n}$ be the public key. Intuitively, as soon as $k_0 \| k_1$ is fixed, $\mathcal{C}$ behaves perfectly as a random permutation as $\mathcal{P}$ is. Formally, simulator $\mathcal{S}$ uses oracle $\mathcal{R}$ to respond with $Y = \mathcal{R}(X \oplus k_0) \oplus k_1$ on a forward query X; and uses its oracle $\mathcal{R}$ to respond with $X = \mathcal{R}^{-1}(Y \oplus k_1) \oplus k_0$ on an inverse query Y. By construction, all queries made by the distinguisher to $\mathcal{S}$ are exactly in correspondence with the random primitive $\mathcal{R}$ and D cannot distinguish.

Now, for $r > 1$, the proof is not much different, although the simulator needs to do some more bookkeeping. It responds randomly at every query, except when it completes a chain, an evaluation $\mathrm{EM}_r(K, p)$, in which case it adapts its response to fit the random oracle. Note that, as the key is fixed, it can be considered constant, and different EM_r evaluations never collide somewhere in the middle. In other words, for any $i \in \{1, \ldots, r\}$ the following holds: if π_i denotes the permutation in the i-th round, then one input-output-tuple of π_i corresponds to exactly one $\mathcal{C}(K, \cdot)$ evaluation, and vice versa. □

We note that EM_1 is *not* iff-secure. Briefly, let $\mathcal{S}$ be any simulator making at most $q_{\mathcal{S}}$ queries. We construct a distinguisher D as follows. Here, $\mathcal{O}_1$ denotes its composed oracle ($\mathcal{C}$ or $\mathcal{R}$) and $\mathcal{O}_2$ its primitive oracle ($\mathcal{P}$ or $\mathcal{S}$). Firstly, D chooses arbitrary key $k_0 \| k_1$ and message M, and queries $Y \leftarrow \mathcal{O}_2(M \oplus k_0)$ and $C \leftarrow \mathcal{O}_1(k_0 \| k_1, M)$. Then, if $C = Y \oplus k_1$, then D outputs 1, otherwise it outputs 0. Note that $C = Y \oplus k_1$ holds with probability 1 in the real world, and with probability $1/2^n$ in the ideal world (as in this setting the simulator does not know k_1). Using Thm. 4, this renders a separation between iff-KK and iff, as already mentioned in Sect. 4.

Acknowledgments. This work has been funded in part by the IAP Program P6/26 BCRYPT of the Belgian State (Belgian Science Policy), in part by the European Commission through the ICT program under contract ICT-2007-216676 ECRYPT II, and in part by the Research Council K.U.Leuven: GOA TENSE. Elena Andreeva is supported by a Postdoctoral Fellowship from the Flemish Research Foundation (FWO-Vlaanderen). Bart Mennink is supported by a Ph.D. Fellowship from the Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen).

References

1. Andreeva, E., Mennink, B., Preneel, B.: On the indifferentiability of the Grøstl hash function. In: Security and Cryptography for Networks 2010. LNCS, vol. 6280, pp. 88–105. Springer, Heidelberg (2010)
2. Bellare, M., Ristenpart, T.: Multi-property-preserving hash domain extension and the EMD Transform. In: ASIACRYPT 2006. LNCS, vol. 4284, pp. 299–314. Springer, Heidelberg (2006)
3. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: On the indifferentiability of the Sponge construction. In: EUROCRYPT 2008. LNCS, vol. 4965, pp. 181–197. Springer, Heidelberg (2008)
4. Bhattacharyya, R., Mandal, A., Nandi, M.: Security analysis of the mode of JH hash function. In: FSE 2010. LNCS, vol. 6147, pp. 168–191. Springer, Heidelberg (2010)
5. Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., Shamir, A.: Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. In: EUROCRYPT 2010. LNCS, vol. 6110, pp. 299–319. Springer, Heidelberg (2010)
6. Biryukov, A., Khovratovich, D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: ASIACRYPT 2009. LNCS, vol. 5912, pp. 1–18. Springer, Heidelberg (2009)
7. Biryukov, A., Khovratovich, D., Nikolic, I.: Distinguisher and related-key attack on the full AES-256. In: CRYPTO 2009. LNCS, vol. 5677, pp. 231–249. Springer, Heidelberg (2009)
8. Bogdanov, A., Khovratovich, D., Rechberger, C.: Biclique cryptanalysis of the full AES. In: ASIACRYPT 2011. LNCS, vol. 7073, pp. 344–371. Springer, Heidelberg (2011)
9. Bogdanov, A., Knudsen, L.R., Leander, G., Standaert, F.X., Steinberger, J., Tischhauser, E.: Key-alternating ciphers in a provable setting: Encryption using a small number of public permutations. In: EUROCRYPT 2012. LNCS, vol. 7237, pp. 45–62. Springer, Heidelberg (2012)
10. Coron, J.S., Patarin, J., Seurin, Y.: The random oracle model and the ideal cipher model are equivalent. In: CRYPTO 2008. LNCS, vol. 5157, pp. 1–20. Springer, Heidelberg (2008)
11. Coron, J.S., Dodis, Y., Malinaud, C., Puniya, P.: Merkle-Damgård revisited: How to construct a hash function. In: CRYPTO 2005. LNCS, vol. 3621, pp. 430–448. Springer, Heidelberg (2005)
12. Daemen, J., Govaerts, R., Vandewalle, J.: Correlation matrices. In: FSE 1994. LNCS, vol. 1008, pp. 275–285. Springer, Heidelberg (1996)
13. Daemen, J., Rijmen, V.: The wide trail design strategy. In: IMA Int. Conf. 2001. LNCS, vol. 2260, pp. 222–238. Springer, Heidelberg (2001)
14. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Springer (2002)
15. Dodis, Y., Puniya, P.: On the relation between the ideal cipher and the random oracle models. In: TCC 2006. LNCS, vol. 3876, pp. 184–206. Springer, Heidelberg (2006)
16. Dodis, Y., Ristenpart, T., Shrimpton, T.: Salvaging Merkle-Damgård for practical applications. In: EUROCRYPT 2009. LNCS, vol. 5479, pp. 371–388. Springer, Heidelberg (2009)
17. Dong, L., Wu, W., Wu, S., Zou, J.: Known-key distinguisher on round-reduced 3D block cipher. In: WISA 2011. LNCS, vol. 7115, pp. 55–69. Springer, Heidelberg (2011)

18. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. In: ASIACRYPT '91. LNCS, vol. 739, pp. 201–224. Springer, Heidelberg (1991)
19. Hirose, S.: Some plausible constructions of double-block-length hash functions. In: FSE 2006. LNCS, vol. 4047, pp. 210–225. Springer, Heidelberg (2006)
20. Hirose, S., Park, J., Yun, A.: A simple variant of the Merkle-Damgård scheme with a permutation. In: ASIACRYPT 2007. LNCS, vol. 4833, pp. 113–129. Springer, Heidelberg (2007)
21. Hoang, V.T., Rogaway, P.: On generalized Feistel networks. In: CRYPTO 2010. LNCS, vol. 6223, pp. 613–630. Springer, Heidelberg (2010)
22. Holenstein, T., Künzler, R., Tessaro, S.: The equivalence of the random oracle model and the ideal cipher model, revisited. In: ACM Symposium on Theory of Computing, STOC. pp. 89–98. ACM, San Jose, CA, USA (2011)
23. Jetchev, D., Özen, O., Stam, M.: Collisions are not incidental: A compression function exploiting discrete geometry. In: TCC 2012. LNCS, vol. 7194, pp. 303–320. Springer, Heidelberg (2012)
24. Knudsen, L.: Block ciphers - the basics (May 2011), eCRYPT II Summer School on Design and Security of Cryptographic Algorithms and Devices, Invited talk, Albena, Bulgaria
25. Knudsen, L., Rijmen, V.: Known-key distinguishers for some block ciphers. In: ASIACRYPT 2007. LNCS, vol. 4833, pp. 315–324. Springer, Heidelberg (2007)
26. Lai, X., Massey, J.: Hash function based on block ciphers. In: EUROCRYPT '92. LNCS, vol. 658, pp. 55–70. Springer, Heidelberg (1992)
27. Luby, M., Rackoff, C.: How to construct pseudorandom permutations from pseudorandom functions. SIAM Journal of Computing 17(2), 373–386 (1988)
28. Mandal, A., Patarin, J., Seurin, Y.: On the public indifferentiability and correlation intractability of the 6-round Feistel construction. In: TCC 2012. LNCS, vol. 7194, pp. 285–302. Springer, Heidelberg (2012)
29. Maurer, U., Renner, R., Holenstein, C.: Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In: TCC 2004. LNCS, vol. 2951, pp. 21–39. Springer, Heidelberg (2004)
30. Maurer, U.M.: A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generator. In: EUROCRYPT 1992. LNCS, vol. 658, pp. 239–255. Springer, Heidelberg (1992)
31. Mennink, B.: Optimal collision security in double block length hashing with single length key. In: ASIACRYPT 2012. LNCS, vol. 7658, pp. 526–543. Springer, Heidelberg (2012)
32. Mennink, B., Preneel, B.: Hash functions based on three permutations: A generic security analysis. In: CRYPTO 2012. LNCS, vol. 7417, pp. 330–347. Springer, Heidelberg (2012)
33. Meyer, C., Schilling, M.: Secure program load with manipulation detection code. In: Proc. Securicom. pp. 111–130 (1988)
34. Minier, M., Phan, R.C.W., Pousse, B.: Distinguishers for ciphers and known key attack against Rijndael with large blocks. In: AFRICACRYPT 2009. LNCS, vol. 5580, pp. 60–76. Springer, Heidelberg (2009)
35. Nakahara Jr., J.: New impossible differential and known-key distinguishers for the 3D cipher. In: ISPEC 2011. LNCS, vol. 6672, pp. 208–221. Springer, Heidelberg (2011)
36. Naor, M., Reingold, O.: On the construction of pseudorandom permutations: Luby-Rackoff revisited. Journal of Cryptology 12(1), 2966 (1999)

37. Nikolic, I., Pieprzyk, J., Sokolowski, P., Steinfeld, R.: Known and chosen key differential distinguishers for block ciphers. In: ICISC 2010. LNCS, vol. 6829, pp. 29–48. Springer, Heidelberg (2010)
38. Patarin, J.: Pseudorandom permutations based on the DES scheme. In: EUROCODE 1990. LNCS, vol. 514, pp. 193–204. Springer, Heidelberg (1990)
39. Patarin, J.: New results on pseudorandom permutation generators based on the DES scheme. In: CRYPTO 1991. LNCS, vol. 576, pp. 301–312. Springer, Heidelberg (1991)
40. Patarin, J.: About Feistel schemes with six (or more) rounds. In: FSE 1998. LNCS, vol. 1372, p. 103121. Springer, Heidelberg (1998)
41. Patarin, J.: Security of random Feistel schemes with 5 or more rounds. In: CRYPTO 2004. LNCS, vol. 3152, p. 106122. Springer, Heidelberg (2004)
42. Preneel, B., Govaerts, R., Vandewalle, J.: Hash functions based on block ciphers: A synthetic approach. In: CRYPTO '93. LNCS, vol. 773, pp. 368–378. Springer, Heidelberg (1993)
43. Rogaway, P., Steinberger, J.: Constructing cryptographic hash functions from fixed-key blockciphers. In: CRYPTO 2008. LNCS, vol. 5157, pp. 433–450. Springer, Heidelberg (2008)
44. Sasaki, Y.: Known-key attacks on Rijndael with large blocks and strengthening *ShiftRow* parameter. In: IWSEC 2010. LNCS, vol. 6434, pp. 301–315. Springer, Heidelberg (2010)
45. Sasaki, Y.: Known-key attacks on Rijndael with large blocks and strengthening *ShiftRow* parameter. IEICE Transactions 95-A(1), 21–28 (2012)
46. Sasaki, Y., Emami, S., Hong, D., Kumar, A.: Improved known-key distinguishers on Feistel-SP ciphers and application to Camellia. In: ACISP 2011. LNCS, vol. 7372, pp. 87–100. Springer, Heidelberg (2012)
47. Sasaki, Y., Yasuda, K.: Known-key distinguishers on 11-round Feistel and collision attacks on its hashing modes. In: FSE 2011. LNCS, vol. 6733, pp. 397–415. Springer, Heidelberg (2011)
48. Shrimpton, T., Stam, M.: Building a collision-resistant compression function from non-compressing primitives. In: ICALP (2) 2008. LNCS, vol. 5126, pp. 643–654. Springer, Heidelberg (2008)
49. Smith, J.: The design of Lucifer: a cryptographic device for data communications. IBM Research Report RC 3326 (1971)
50. Stam, M.: Blockcipher-based hashing revisited. In: FSE 2009. LNCS, vol. 5665, pp. 67–83. Springer, Heidelberg (2009)
51. Steinberger, J.: Improved security bounds for key-alternating ciphers via Hellinger distance. Cryptology ePrint Archive, Report 2012/481 (2012)
52. Vaudenay, S.: Decorrelation: A theory for block cipher security. Journal of Cryptology 16(1), 249–286 (2003)
53. Yoneyama, K., Miyagawa, S., Ohta, K.: Leaky random oracle. IEICE Transactions 92-A(1), 1795–1807 (2009)
54. Zheng, Y., Matsumoto, T., Imai, H.: On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In: CRYPTO '89. LNCS, vol. 435, pp. 461–480. Springer, Heidelberg (1989)