Impossibility of Indifferentiable Iterated Blockciphers from 3 or Less Primitive Calls

Speaker: Yaobin Shen
Chun Guo Lei Wang Dongdai Lin

EUROCRYPT 2023 – April 26, 2023

Section 1

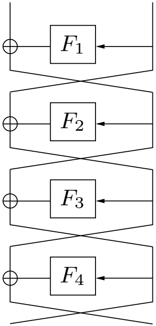
Background

Iterated blockciphers

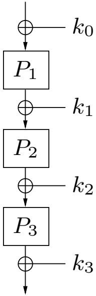
- Virtually all modern blockciphers are iterated blockciphers

Iterated blockciphers

- Virtually all modern blockciphers are iterated blockciphers
- Compositions of "rounds"/simpler blockciphers



Feistel network: DES, SIMON, etc.
Provable security up to $2^{n/2}$ queries.



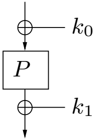
Iterated Even-Mansour (IEM): AES, Skinny, etc.
Provable security up to $2^{3n/4}$ queries.

We ask: are there lower bounds?

- How many random function/permutation-calls are necessary for a “non-trivial” iterated blockcipher?

We ask: are there lower bounds?

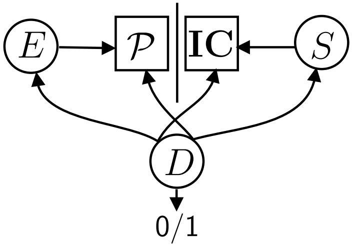
- How many random function/permutation-calls are necessary for a "non-trivial" iterated blockcipher?
- **Indistinguishability** from a random permutation: 1 call to a public permutation



Even-Mansour cipher [EM97]: provable security up to $2^{n/2}$ queries

We ask: are there lower bounds?

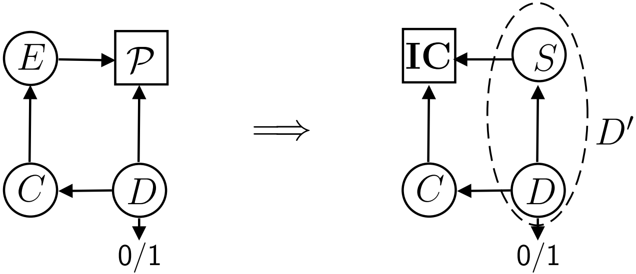
- How many random function/permutation-calls are necessary for a "non-trivial" iterated blockcipher?
- **Indistinguishability** from a random permutation: 1 call to a public permutation
- **Indifferentiability** from an ideal cipher?



Indifferentiability of blockciphers

Why indifferentiability?

- Because of the composition theorem: $C^{E^{\mathcal{P}}}$ using an indifferentiable blockcipher is as secure as $C^{\mathbf{IC}}$.
- Limitations: single-stage [RSS11, BBM13], complexity blow-up [DRST12, DGHM13].

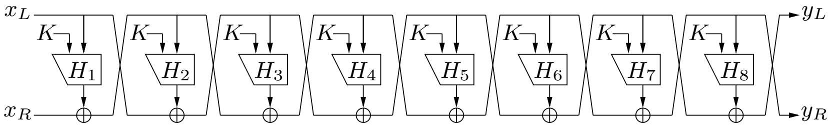


Adversary D against $C^{E^{\mathcal{P}}}$ $\Longrightarrow$ Adversary $D' = (D, S)$ constitutes an adversary against $C^{\mathbf{IC}}$

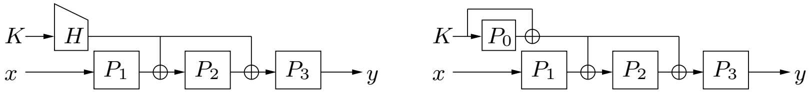
Indifferentiability of blockciphers

We had fruitful positive results:

- Key-prepended Feistel ciphers [CPS08, HKT11, DKT16, DS16]
- Iterated Even-Mansour ciphers [ABD$^+$13, LS13, DSST17, GL16]
- Confusion-diffusion networks [DSSL16]



8-round Key-prepended Feistel cipher [DS16]



3-round iterated Even-Mansour with an idealized key derivation [GL16]

Indifferentiability of blockciphers

Fruitful positive results

- Key-prepended Feistel ciphers [CPS08, HKT11, DKT16, DS16]
- Iterated Even-Mansour ciphers [ABD+13, LS13, DSST17, GL16]
- Confusion-diffusion networks [DSSL16]

But no general lower bounds

- Only specific lower bounds for specific constructions
- Key-prepended Feistel: at least 6 rounds (6 calls to random functions) [CPS08]
- Iterated Even-Mansour with key derivation: at least 3 rounds (4 calls to random permutations or functions) [ABD+13, GL16]
- Iterated Even-Mansour without key derivation: 5 rounds (5 calls to random permutations) necessary and sufficient [LS13, DSST17]

Back to the question

- How many random function/permutation-calls are necessary for a "non-trivial" iterated blockcipher...
- What does it mean by "non-trivial"?

Back to the question

- How many random function/permutation-calls are necessary for a "non-trivial" iterated blockcipher...
- What does it mean by "non-trivial"?
  - An ideal cipher with n-bit blocks is an exponential number of n-bit random permutations

Back to the question

- How many random function/permutation-calls are necessary for a "non-trivial" iterated blockcipher...
- What does it mean by "non-trivial"?
  - An ideal cipher with n-bit blocks is an exponential number of n-bit random permutations
  - Trivial case: we already have so many n-bit random permutations!

Back to the question

- How many random function/permutation-calls are necessary for a “non-trivial” iterated blockcipher...
- What does it mean by “non-trivial”?
  - An ideal cipher with n-bit blocks is an exponential number of n-bit random permutations
  - Trivial case: we already have so many n-bit random permutations!
- Oracle $\mathcal{P} = (\mathbf{P}_1, \mathbf{P}_2, ..., \mathbf{P}_{|\mathcal{I}|})$
  - $\mathbf{P}_i : \{0,1\}^{(m(i))} \to \{0,1\}^{(m(i))}$ is a random permutation of width $m(i) = \text{poly}(n)$
  - $\mathcal{I} = \mathcal{I}_{\le n} \sqcup \mathcal{I}_{>n}$, where $m(i) \le n$ iff. $i \in \mathcal{I}_{\le n}$

Back to the question

- How many random function/permutation-calls are necessary for a "non-trivial" iterated blockcipher...
- What does it mean by "non-trivial"?
  - An ideal cipher with n-bit blocks is an exponential number of n-bit random permutations
  - Trivial case: we already have so many n-bit random permutations!
- Oracle $\mathcal{P} = (\mathbf{P}_1, \mathbf{P}_2, ..., \mathbf{P}_{|\mathcal{I}|})$
  - $\mathbf{P}_i : \{0,1\}^{(m(i))} \to \{0,1\}^{(m(i))}$ is a random permutation of width $m(i) = \text{poly}(n)$
  - $\mathcal{I} = \mathcal{I}_{\leq n} \sqcup \mathcal{I}_{>n}$, where $m(i) \leq n$ iff. $i \in \mathcal{I}_{\leq n}$
  - Avoid trivial results: $|\mathcal{I}_{\leq n}| = O(\text{poly}(n))$

Back to the question

- How many random function/permutation-calls are necessary for a "non-trivial" iterated blockcipher...
- What does it mean by "non-trivial"?
  - An ideal cipher with n-bit blocks is an exponential number of n-bit random permutations
  - Trivial case: we already have so many n-bit random permutations!
- Oracle $\mathcal{P} = (\mathbf{P}_1, \mathbf{P}_2, ..., \mathbf{P}_{|\mathcal{I}|})$
  - $\mathbf{P}_i : \{0,1\}^{(m(i))} \to \{0,1\}^{(m(i))}$ is a random permutation of width $m(i) = \text{poly}(n)$
  - $\mathcal{I} = \mathcal{I}_{\leq n} \sqcup \mathcal{I}_{>n}$, where $m(i) \leq n$ iff. $i \in \mathcal{I}_{\leq n}$
  - Avoid trivial results: $|\mathcal{I}_{\leq n}| = O(\text{poly}(n))$
  - Can have exponentially many large permutations: $|\mathcal{I}_{>n}| = 2^{\text{poly}(n)}$: this offers indifferentiable functions [CLL19] and injections [BF18].

Back to the question

- How many random function/permutation-calls are necessary for a "non-trivial" iterated blockcipher...
- What does it mean by "non-trivial"?
  - An ideal cipher with n-bit blocks is an exponential number of n-bit random permutations
  - Trivial case: we already have so many n-bit random permutations!
- Oracle $\mathcal{P} = (\mathbf{P}_1, \mathbf{P}_2, ..., \mathbf{P}_{|\mathcal{I}|})$
  - $\mathbf{P}_i : \{0,1\}^{(m(i))} \to \{0,1\}^{(m(i))}$ is a random permutation of width $m(i) = \mathsf{poly}(n)$
  - $\mathcal{I} = \mathcal{I}_{\leq n} \sqcup \mathcal{I}_{>n}$, where $m(i) \leq n$ iff. $i \in \mathcal{I}_{\leq n}$
  - Avoid trivial results: $|\mathcal{I}_{\leq n}| = O(\mathsf{poly}(n))$
  - Can have exponentially many large permutations: $|\mathcal{I}_{>n}| = 2^{\mathsf{poly}(n)}$: this offers indifferentiable functions [CLL19] and injections [BF18].
  - Input: (i, δ, z), $(i, \delta) \in \mathcal{I} \times \{+, -\}$ for index and direction, $z \in \{0,1\}^{m(i)}$ for input

Back to the question

- How many random function/permutation-calls are necessary for a "non-trivial" iterated blockcipher...
- What does it mean by "non-trivial"?
  - An ideal cipher with n-bit blocks is an exponential number of n-bit random permutations
  - Trivial case: we already have so many n-bit random permutations!
- Oracle $\mathcal{P} = (\mathbf{P}_1, \mathbf{P}_2, ..., \mathbf{P}_{|\mathcal{I}|})$
  - $\mathbf{P}_i : \{0,1\}^{(m(i))} \to \{0,1\}^{(m(i))}$ is a random permutation of width $m(i) = \text{poly}(n)$
  - $\mathcal{I} = \mathcal{I}_{\le n} \sqcup \mathcal{I}_{>n}$, where $m(i) \le n$ iff. $i \in \mathcal{I}_{\le n}$
  - Avoid trivial results: $|\mathcal{I}_{\le n}| = O(\text{poly}(n))$
  - Can have exponentially many large permutations: $|\mathcal{I}_{>n}| = 2^{\text{poly}(n)}$: this offers indifferentiable functions [CLL19] and injections [BF18].
  - Input: (i, δ, z), $(i, \delta) \in \mathcal{I} \times \{+, -\}$ for index and direction, $z \in \{0,1\}^{m(i)}$ for input
    - *BTW: when $|\mathcal{I}_{\le n}| = 2^{poly(n)}$, it seems our impossibility result on 1-call blockciphers $E1^{\mathcal{P}}$ still holds, but our differentiators on $E2^{\mathcal{P}}$ and $E3^{\mathcal{P}}$ don't work. This matches existing indifferentiable key-length extension results [CDMS10, GLL16].*

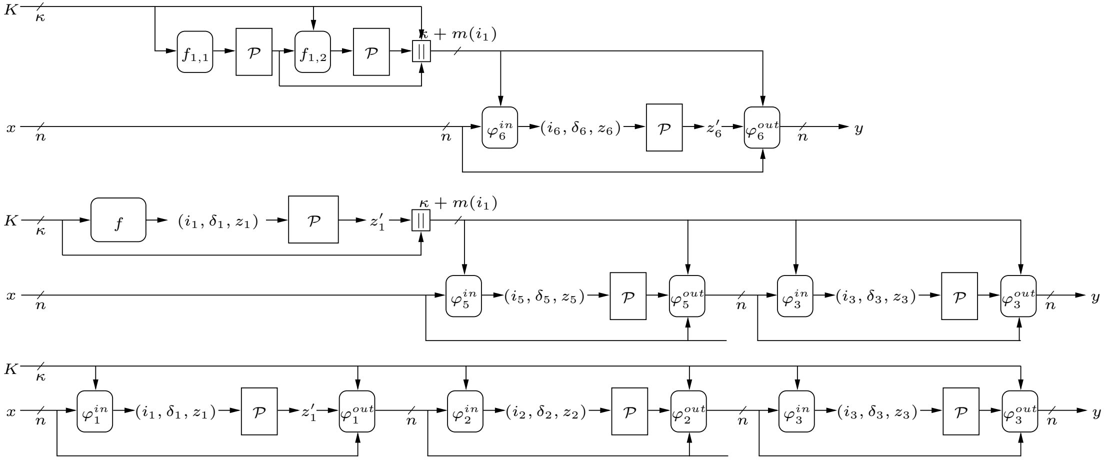
Section 2

Contributions

Main results: first general lower bound

- (Informal) No iterated blockcipher making 3 or less calls to the oracle $\mathcal{P}$ is statistically indifferentiable from ideal ciphers.
  - The 4-call positive result [GL16] is thus optimal.

3-call iterated blockcipher $E3^{\mathcal{P}} : \{0,1\}^{\kappa} \times \{0,1\}^n \to \{0,1\}^n$



Section 3

Results in detail

Four fundamental properties of a blockcipher oracle procedure $E^{\mathcal{P}}$

- By the definition of the notion of blockciphers:
  1. **Efficient invertibility**: there is a corresponding oracle procedure $(E^{-1})^{\mathcal{P}}$ computing its inverse;
  2. **Deterministic**: evaluating $E^{\mathcal{P}}(K,x) \to y$ and $(E^{-1})^{\mathcal{P}}(K,y)$ always yield the same transcript of $\mathcal{P}$-queries and responses.

Four fundamental properties of a blockcipher oracle procedure $E^{\mathcal{P}}$

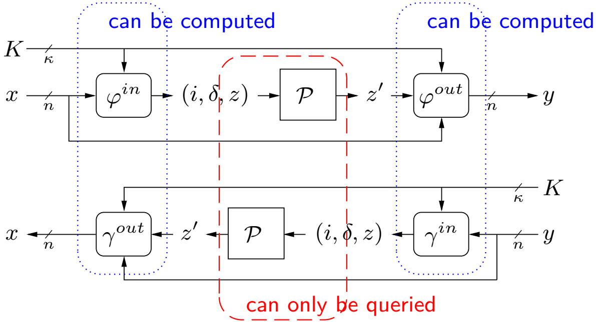
- By the definition of the notion of blockciphers:
  1. **Efficient invertibility**: there is a corresponding oracle procedure $(E^{-1})^{\mathcal{P}}$ computing its inverse;
  2. **Deterministic**: evaluating $E^{\mathcal{P}}(K,x) \to y$ and $(E^{-1})^{\mathcal{P}}(K,y)$ always yield the same transcript of $\mathcal{P}$-queries and responses.
- By fixed descriptions of oracle procedures: sub-procedures in $E^{\mathcal{P}}$ are **oracle-independent**.

Four fundamental properties of a blockcipher oracle procedure $E^{\mathcal{P}}$

- By the definition of the notion of blockciphers:
  1. **Efficient invertibility**: there is a corresponding oracle procedure $(E^{-1})^{\mathcal{P}}$ computing its inverse;
  2. **Deterministic**: evaluating $E^{\mathcal{P}}(K,x) \to y$ and $(E^{-1})^{\mathcal{P}}(K,y)$ always yield the same transcript of $\mathcal{P}$-queries and responses.
- By fixed descriptions of oracle procedures: sub-procedures in $E^{\mathcal{P}}$ are **oracle-independent**.
- **Non-degeneracy**: no encipherment $E^{\mathcal{P}}(K,x)$ can be approximately computed using less $\mathcal{P}$ calls than $E^{\mathcal{P}}$.

Model for 1-call cipher $E1$

- 1-call blockcipher/round $E1^{\mathcal{P}}(K,x) := \varphi^{out}\big(K, \mathcal{P}(\varphi^{in}(K,x)), x\big)$: $K \in \mathcal{K}$, $x \in \{0,1\}^n$
- Efficient inversion within 1 $\mathcal{P}$-call: $(E1^{-1})^{\mathcal{P}}(K,y) := \gamma^{out}\big(K, \mathcal{P}(\gamma^{in}(K,y)), y\big)$ for two other input and output functions γ^{in} and γ^{out}



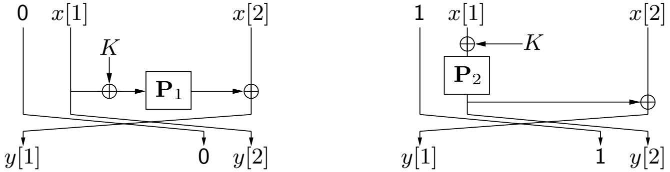
Full characterization of 1-call cipher $E1$

The *Fundamental Properties* already ensure a number of non-trivial properties (on oracle procedures of blockciphers):

1. Inv-freeness and its oracle-independence.
2. Properties of inv-free $E1^{\mathcal{P}}(K, x)$.
3. Properties of non-inv-free $E1^{\mathcal{P}}(K, x)$.

Full characterization of 1-call cipher $E1$

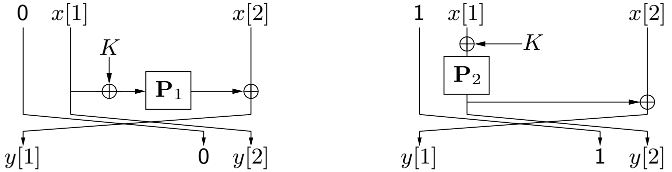
1. Inv-freeness and its oracle-independence
   - Inverse-free encipherments: $E1^{\mathcal{P}}(K,x) \to y$ and $(E1^{-1})^{\mathcal{P}}(K,y) \to x$ call $\mathcal{P}(i,\delta,\star)$ on the same direction δ.
   - Otherwise $E1^{\mathcal{P}}(K,x)$ is non-inverse-free



2. Properties of inv-free $E1^{\mathcal{P}}(K,x)$
3. Properties of non-inv-free $E1^{\mathcal{P}}(K,x)$

Full characterization of 1-call cipher $E1$

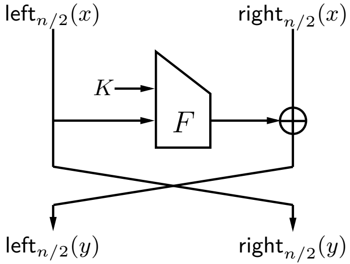
1. Inv-freeness and its oracle-independence
   - Inverse-free encipherments: $E1^{\mathcal{P}}(K,x) \to y$ and $(E1^{-1})^{\mathcal{P}}(K,y) \to x$ call $\mathcal{P}(i,\delta,\star)$ on the same direction δ.
   - Otherwise $E1^{\mathcal{P}}(K,x)$ is non-inverse-free



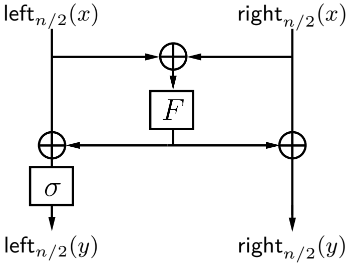
   - Observation: *in $E1^{\mathcal{P}}$, inv-freeness cannot depend on the oracle $\mathcal{P}$*, i.e., one can decide if an encipherment $E1^{\mathcal{P}}(K,x)$ is inv-free without querying $\mathcal{P}$.
2. Properties of inv-free $E1^{\mathcal{P}}(K,x)$
3. Properties of non-inv-free $E1^{\mathcal{P}}(K,x)$

Full characterization of 1-call cipher $E1$

1. Inv-freeness and its oracle-independence
2. Properties of inv-free $E1^{\mathcal{P}}(K, x)$



Feistel:
$\text{left}(x) = \text{right}(y)$,
$2^{n/2}$ distinct (K, x) call same $F\Big(K \| \text{left}(x)\Big)$

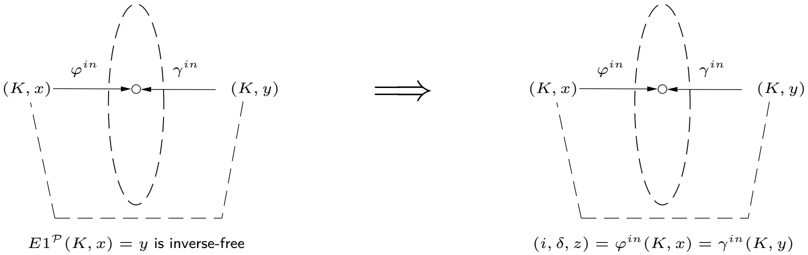


Lai-Massey:
$\text{left}(x) \oplus \text{right}(x) = \sigma^{-1}(\text{left}(y)) \oplus \text{right}(y)$,
$2^{n/2}$ distinct (K, x) call same $F\Big(\text{left}(x) \oplus \text{right}(x)$

3. Properties of non-inv-free $E1^{\mathcal{P}}(K, x)$

Full characterization of 1-call cipher $E1$

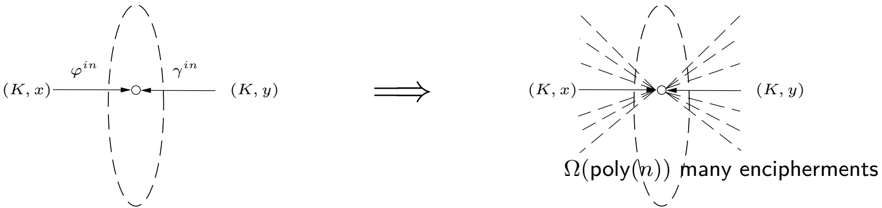
1. Inv-freeness and its oracle-independence
2. Properties of inv-free $E1^{\mathcal{P}}(K,x)$



3. Properties of non-inv-free $E1^{\mathcal{P}}(K,x)$

Full characterization of 1-call cipher $E1$

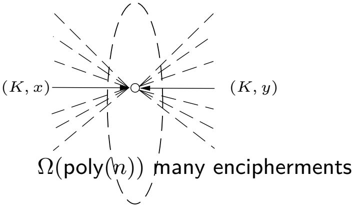
1. Inv-freeness and its oracle-independence
2. Properties of inv-free $E1^{\mathcal{P}}(K, x)$



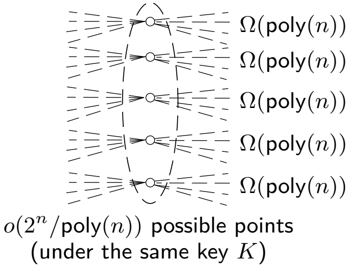
3. Properties of non-inv-free $E1^{\mathcal{P}}(K, x)$

Full characterization of 1-call cipher $E1$

1. Inv-freeness and its oracle-independence
2. Properties of inv-free $E1^{\mathcal{P}}(K,x)$



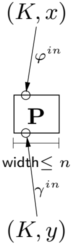
$\Longrightarrow$



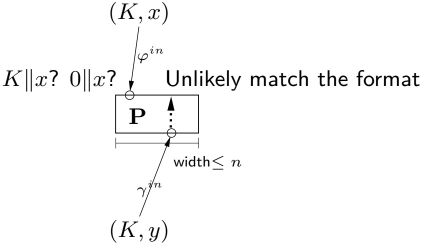
3. Properties of non-inv-free $E1^{\mathcal{P}}(K,x)$

Full characterization of 1-call cipher $E1$

1. Inv-freeness and its oracle-independence
2. Properties of inv-free $E1^{\mathcal{P}}(K, x)$
3. Properties of non-inv-free $E1^{\mathcal{P}}(K, x)$



$(i, \delta, z) \in \{+, -\} \times \mathcal{I}_{\leq n} \times \{0,1\}^{m(i)}$:
At most $2^{n+1}|\mathcal{I}_{\leq n}|$ possibilities



Attack $E1^{\mathcal{P}} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

With the above properties, we are able to bump into our differentiator $D1$ on $E1^{\mathcal{P}}$. In detail, the cipher $E1^{\mathcal{P}} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ may fall into two cases.

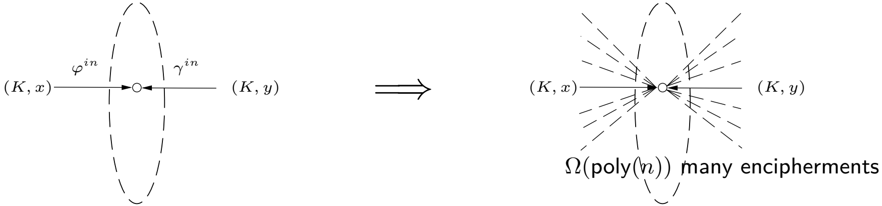
Condition: $|\mathcal{K}| \geq 2|\mathcal{I}_{\leq n}| + 1 = O(\text{poly}(n))$.

Attack $E1^{\mathcal{P}} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

With the above properties, we are able to bump into our differentiator $D1$ on $E1^{\mathcal{P}}$. In detail, the cipher $E1^{\mathcal{P}} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ may fall into two cases.

Condition: $|\mathcal{K}| \geq 2|\mathcal{I}_{\leq n}| + 1 = O(\text{poly}(n))$.

- Case 1: there exists at least 1 inv-free encipherment $E1^{\mathcal{P}}(K, x)$.
  As discussed, there are $t = \Omega(\text{poly}(n))$ distinct inv-free $E1^{\mathcal{P}}(K, x_1), ..., E1^{\mathcal{P}}(K, x_t)$ with $\varphi^{in}(K, x_1) = ... = \varphi^{in}(K, x_t) = (i, \delta, z)$. Thus, the restriction of $E1^{\mathcal{P}}(K, \cdot)$ to $\{x_1, ..., x_t\}$ is a bijection defined upon a polynomial-length random string $z' = \mathcal{P}(i, \delta, z)$.

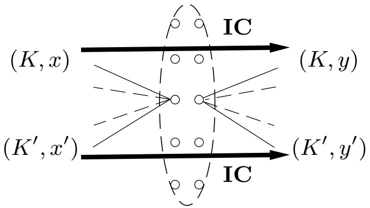


Attack $E1^{\mathcal{P}} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

With the above properties, we are able to bump into our differentiator $D1$ on $E1^{\mathcal{P}}$. In detail, the cipher $E1^{\mathcal{P}} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ may fall into two cases.

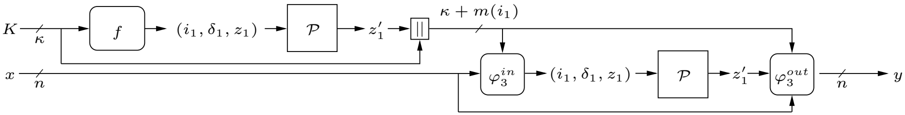
Condition: $|\mathcal{K}| \geq 2|\mathcal{I}_{\leq n}| + 1 = O(\text{poly}(n))$.

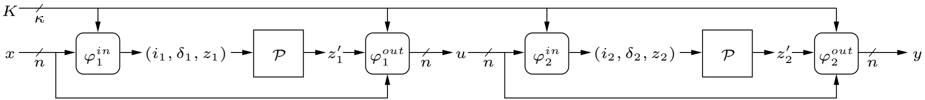
- Case 2: $E1^{\mathcal{P}}(K,x)$ is non-inv-free for all $(K,x) \in \mathcal{K} \times \{0,1\}^n$.
  The pigeonhole principle guarantees $\exists (K,x),(K',x') \in \mathcal{K} \times \{0,1\}^n$ with collision $\varphi^{in}(K,x) = \varphi^{in}(K',x')$ for attack.



width$\leq n$
$\Rightarrow \sharp$ points $\leq |\mathcal{I}_{\leq n}| 2^{n+1}$

2-call iterated blockcipher $E2^{\mathcal{P}}(K, x)$: $K \in \mathcal{K}$, $x \in \{0,1\}^n$





2-call iterated blockcipher $E2^{\mathcal{P}}(K, x)$: $K \in \mathcal{K}$, $x \in \{0,1\}^n$

- Key space can be partitioned: $\mathcal{K} = \mathcal{K}^{(0)} \sqcup \mathcal{K}^{(1)}$

2-call iterated blockcipher $E2^{\mathcal{P}}(K,x)$: $K \in \mathcal{K}$, $x \in \{0,1\}^n$

- Key space can be partitioned: $\mathcal{K} = \mathcal{K}^{(0)} \sqcup \mathcal{K}^{(1)}$
- For all $K \in \mathcal{K}^{(1)}$: $E2^{\mathcal{P}}(K,x) = \Pi_3^{\mathcal{P}}\big(K \| \mathsf{kd}^{\mathcal{P}}(K), x\big)$ invokes a 1-call key derivation function $\mathsf{kd}^{\mathcal{P}}$
  - $E2^{\mathcal{P}}(K,x) = \Pi_3^{\mathcal{P}}\big(K \| \mathsf{kd}^{\mathcal{P}}(K), x\big)$ for a 1-call function $\mathsf{kd}^{\mathcal{P}} : \{0,1\}^{\kappa} \to \{0,1\}^{m_{max}}$ and a 1-call cipher $\Pi_3^{\mathcal{P}} : \{0,1\}^{\kappa+m_{max}} \times \{0,1\}^n \to \{0,1\}^n$;
  - $\mathsf{kd}^{\mathcal{P}}(K) = \mathcal{P}\big(f(K)\big)$ for another oracle-independent function f
  - $\Pi_3^{\mathcal{P}}\big(K \| \mathsf{kd}^{\mathcal{P}}(K), x\big) = \varphi_3^{out}\big(K, \mathcal{P}(\varphi_3^{in}(K,x)), x\big)$

2-call iterated blockcipher $E2^{\mathcal{P}}(K,x)$: $K \in \mathcal{K}$, $x \in \{0,1\}^n$

- Key space can be partitioned: $\mathcal{K} = \mathcal{K}^{(0)} \sqcup \mathcal{K}^{(1)}$
- For all $K \in \mathcal{K}^{(1)}$: $E2^{\mathcal{P}}(K,x) = \Pi_3^{\mathcal{P}}\big(K \| \mathsf{kd}^{\mathcal{P}}(K), x\big)$ invokes a 1-call key derivation function $\mathsf{kd}^{\mathcal{P}}$
  - $E2^{\mathcal{P}}(K,x) = \Pi_3^{\mathcal{P}}\big(K \| \mathsf{kd}^{\mathcal{P}}(K), x\big)$ for a 1-call function $\mathsf{kd}^{\mathcal{P}} : \{0,1\}^{\kappa} \to \{0,1\}^{m_{max}}$ and a 1-call cipher $\Pi_3^{\mathcal{P}} : \{0,1\}^{\kappa+m_{max}} \times \{0,1\}^n \to \{0,1\}^n$;
  - $\mathsf{kd}^{\mathcal{P}}(K) = \mathcal{P}\big(f(K)\big)$ for another oracle-independent function f
  - $\Pi_3^{\mathcal{P}}\big(K \| \mathsf{kd}^{\mathcal{P}}(K), x\big) = \varphi_3^{out}\big(K, \mathcal{P}(\varphi_3^{in}(K,x)), x\big)$
- For all $K \in \mathcal{K}^{(0)}$: $E2^{\mathcal{P}}(K,x) = \Pi_2^{\mathcal{P}}\big(K, \Pi_1^{\mathcal{P}}(K,x)\big)$, there is no key derivation in the form of oracle procedures
  - $\Pi_1^{\mathcal{P}}\big(K \| \mathsf{kd}^{\mathcal{P}}(K), x\big) = \varphi_1^{out}\big(K, \mathcal{P}(\varphi_1^{in}(K,x)), x\big)$ and $\Pi_2^{\mathcal{P}}\big(K \| \mathsf{kd}^{\mathcal{P}}(K), x\big) = \varphi_2^{out}\big(K, \mathcal{P}(\varphi_2^{in}(K,x)), x\big)$ are two 1-call ciphers/rounds.

Attack $E2^{\mathcal{P}} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

Built upon our above results on $E1^{\mathcal{P}}$, we further consider our 2-call model $E2^{\mathcal{P}}$.

- Case 1: $E2^{\mathcal{P}}$ invokes kd for sufficiently many keys. (Formally, $|\mathcal{K}^{(1)}| \geq 2|\mathcal{I}_{\leq n}| + 1$.)
  1. We simply pick $\lambda = 2|\mathcal{I}_{\leq n}| + 1$ keys $K_1, ..., K_\lambda \in \mathcal{K}^{(1)}$ and derive subkeys $s_1 = \mathsf{kd}^{\mathcal{P}}(K_1), ..., s_\lambda = \mathsf{kd}^{\mathcal{P}}(K_\lambda)$. This consumes at most $\lambda = O(\mathsf{poly}(n))$ P-queries.
  2. We then view the round $\Pi_3^{\mathcal{P}}$ as a 1-call cipher with keyspace $\{K_1 \| s_1, ..., K_\lambda \| s_\lambda\}$ and apply our differentiator $D1$.
  3. It is thus crucial that $D1$ can break $E1$ with polynomial-keyspace.

Attack $E2^{\mathcal{P}} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

Built upon our above results on $E1^{\mathcal{P}}$, we further consider our 2-call model $E2^{\mathcal{P}}$.

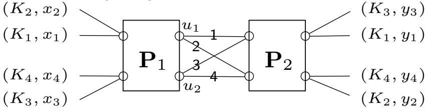
- Case 2 (less obvious): $E2^{\mathcal{P}}(K,x) = \Pi_2^{\mathcal{P}}\big(K, \Pi_1^{\mathcal{P}}(K,x)\big)$ is 2-iteration for most keys.
  1. Starting point: boomerang property
  2. Using graph theory on girth
  3. From boomerang to yoyo
  4. Non-degenerate input functions

Attack $E2^{\mathcal{P}} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

Built upon our above results on $E1^{\mathcal{P}}$, we further consider our 2-call model $E2^{\mathcal{P}}$.

- Case 2 (less obvious): $E2^{\mathcal{P}}(K,x) = \Pi_2^{\mathcal{P}}\big(K, \Pi_1^{\mathcal{P}}(K,x)\big)$ is 2-iteration for most keys.
  1. Starting point: boomerang property
     - In the 2-round Even-Mansour cipher $y = K \oplus \mathbf{P}_2(K \oplus \mathbf{P}_1(K \oplus x))$
     - Computing four distinct pairs $(K_1,u_1),(K_2,u_2),(K_3,u_3),(K_4,u_4)$ inducing two collided inputs to $\mathbf{P}_1^{-1}$ and two collide inputs to $\mathbf{P}_2$.
     - Can compute a 4-tuple of cipher inputs/outputs $\big((K_1,x_1,y_1),\ldots,(K_4,x_4,y_4)\big)$ that has $K_1 \oplus x_1 = K_2 \oplus x_2$, $K_3 \oplus x_3 = K_4 \oplus x_4$; $K_1 \oplus y_1 = K_3 \oplus y_3$, $K_2 \oplus y_2 = K_4 \oplus y_4$.

$u_1 = u_2$, $u_3 = u_4$;
$K_1 \oplus u_1 = K_3 \oplus u_3$, $K_2 \oplus u_2 = K_4 \oplus u_4$

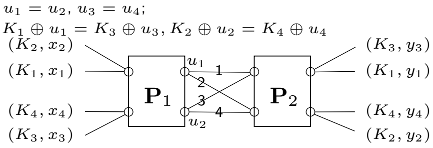


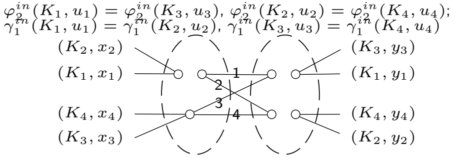
  2. Using graph theory on girth
  3. From boomerang to yoyo

Attack $E2^{\mathcal{P}} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

Built upon our above results on $E1^{\mathcal{P}}$, we further consider our 2-call model $E2^{\mathcal{P}}$.

- Case 2 (less obvious): $E2^{\mathcal{P}}(K,x) = \Pi_2^{\mathcal{P}}\big(K, \Pi_1^{\mathcal{P}}(K,x)\big)$ is 2-iteration for most keys.
  1. Starting point: boomerang property
     - Generalized boomerang: find pairs $(K_1,u_1),(K_2,u_2),(K_3,u_3),(K_4,u_4) \in \mathcal{K}^{(0)} \times \{0,1\}^n$ that induce similar collided $\mathcal{P}$-calls.
     - Can computes a 4-tuple of cipher inputs/outputs $\big((K_1,x_1,y_1),...,(K_4,x_4,y_4)\big)$ that has $\varphi_1^{in}(K_1,u_1) = \varphi_1^{in}(K_2,u_2)$, $\varphi_1^{in}(K_3,u_3) = \varphi_1^{in}(K_4,u_4)$, $\gamma_2^{in}(K_1,u_1) = \gamma_2^{in}(K_3,u_3)$ and $\gamma_2^{in}(K_2,u_2) = \gamma_2^{in}(K_4,u_4)$.



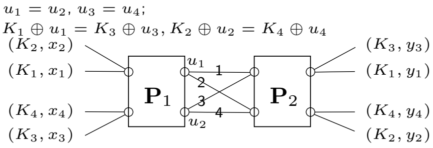


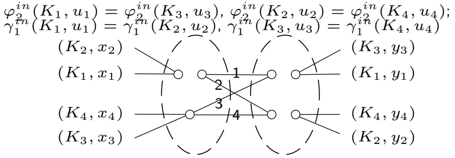
  2. Using graph theory on girth
  3. From boomerang to yoyo

Attack $E2^{\mathcal{P}} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

Built upon our above results on $E1^{\mathcal{P}}$, we further consider our 2-call model $E2^{\mathcal{P}}$.

- Case 2 (less obvious): $E2^{\mathcal{P}}(K,x) = \Pi_2^{\mathcal{P}}\left(K, \Pi_1^{\mathcal{P}}(K,x)\right)$ is 2-iteration for most keys.
  1. Starting point: boomerang property
  2. Using graph theory on girth
     - Existence of $(K_1,u_1),(K_2,u_2),(K_3,u_3),(K_4,u_4) \in \mathcal{K}^{(0)} \times \{0,1\}^n$?
     - A 4-cycle C_4 in a bipartite graph with left and right shore size$\leq |\mathcal{I}_{\leq n}|2^{n+1}$ and $|\mathcal{K}^{(0)}|2^n$ edges
     - Hoory [Hoo02]: when $|\mathcal{K}^{(0)}| = \Theta(2^n)$ (key-length$\approx n$), cycles of length≤ 4 must exist



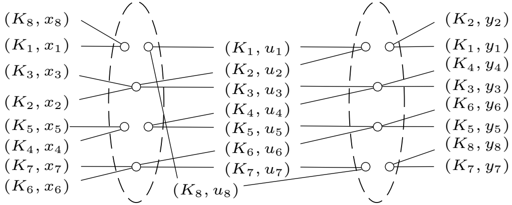


  3. From boomerang to yoyo

Attack $E2^{\mathcal{P}} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

Built upon our above results on $E1^{\mathcal{P}}$, we further consider our 2-call model $E2^{\mathcal{P}}$.

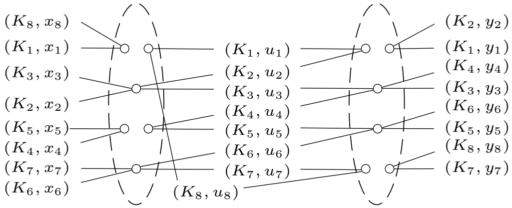
- Case 2 (less obvious): $E2^{\mathcal{P}}(K,x) = \Pi_2^{\mathcal{P}}\left(K, \Pi_1^{\mathcal{P}}(K,x)\right)$ is 2-iteration for most keys.
  1. Starting point: boomerang property
  2. Using graph theory on girth
  3. From boomerang to yoyo
     - But with $|\mathcal{K}^{(0)}| = \Theta(2^n)$, we cannot invoke the attack for $E3^{\mathcal{P}}$ with KDFs!
     - A general yoyo distinguisher [RBH17]: consider longer cycles $C_{2\lambda}$, $\lambda \le n+1$. I.e., find 2λ-tuple $\left((K_1,u_1)\ ,\ldots,(K_{2\lambda},u_{2\lambda})\right)$ with $\varphi_2^{in}(K_1,u_1) = \varphi_2^{in}(K_2,u_2), \gamma_1^{in}(K_2,u_2) = \gamma_1^{in}(K_3,u_3), \varphi_2^{in}(K_3,u_3) = \varphi_2^{in}(K_4,u_4), \gamma_1^{in}(K_4,u_4) = \gamma_1^{in}(K_5,u_5), \ldots, \varphi_2^{in}(K_{2\lambda-1},u_{2\lambda-1}) = \varphi_2^{in}(K_{2\lambda},u_{2\lambda}), \gamma_1^{in}(K_{2\lambda},u_{2\lambda}) = \gamma_1^{in}(K_1,u_1)$.



Attack $E2^{\mathcal{P}} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

Built upon our above results on $E1^{\mathcal{P}}$, we further consider our 2-call model $E2^{\mathcal{P}}$.

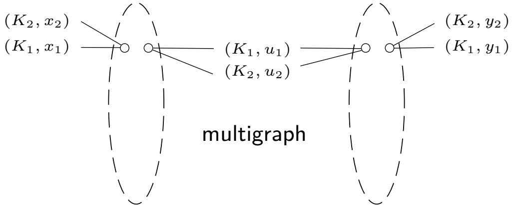
- Case 2 (less obvious): $E2^{\mathcal{P}}(K,x) = \Pi_2^{\mathcal{P}}\big(K, \Pi_1^{\mathcal{P}}(K,x)\big)$ is 2-iteration for most keys.
  1. Starting point: boomerang property
  2. Using graph theory on girth
  3. From boomerang to yoyo
     - Can compute a 2λ-tuple of $E2$ inputs/outputs $\big((K_1,x_1,y_1),...,(K_{2\lambda},x_{2\lambda},y_{2\lambda})\big)$ that has a "cycle of collisions". I.e., $\gamma_2^{in}(K_1,y_1) = \gamma_2^{in}(K_2,y_2), \varphi_1^{in}(K_2,x_2) = \varphi_1^{in}(K_3,x_3),...,\gamma_2^{in}(K_{2\lambda-1},y_{2\lambda-1}) = \gamma_2^{in}(K_{2\lambda},y_{2\lambda}), \varphi_1^{in}(K_{2\lambda},x_{2\lambda}) = \varphi_1^{in}(K_1,x_1)$.
     - By Hoory [Hoo02], $|\mathcal{K}^{(0)}| \geq \Big(6\big(3|\mathcal{I}_{\leq n}|\big)^{\frac{1}{n}} + 3\Big)|\mathcal{I}_{\leq n}| = O(\mathsf{poly}(n))$ suffices!



Attack $E2^{\mathcal{P}} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

Built upon our above results on $E1^{\mathcal{P}}$, we further consider our 2-call model $E2^{\mathcal{P}}$.

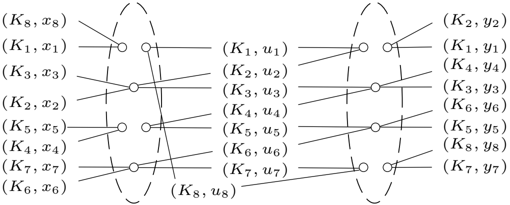
- Case 2 (less obvious): $E2^{\mathcal{P}}(K,x) = \Pi_2^{\mathcal{P}}\left(K, \Pi_1^{\mathcal{P}}(K,x)\right)$ is 2-iteration for most keys.
  1. Starting point: boomerang property
  2. Using graph theory on girth
  3. From boomerang to yoyo
     - Hoory [Hoo02] does not apply when $\mathcal{G}$ is a multigraph, but this implies existence of C_2, which is an even weaker case.



Attack $E2^{\mathcal{P}} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

Built upon our above results on $E1^{\mathcal{P}}$, we further consider our 2-call model $E2^{\mathcal{P}}$.

- Case 2 (less obvious): $E2^{\mathcal{P}}(K,x) = \Pi_2^{\mathcal{P}}\big(K, \Pi_1^{\mathcal{P}}(K,x)\big)$ is 2-iteration for most keys.
  1. Starting point: boomerang property
  2. Using graph theory on girth
  3. From boomerang to yoyo
  + Crucial to restrict our discussion to iterated blockciphers with a clear valid intermediate value set $\{0,1\}^n$: an attacker can pick such a u and compute forward or backward.



3-call iterated blockcipher $E3^{\mathcal{P}} : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$

- Partition the key space: $\mathcal{K} = \mathcal{K}^{(0)} \sqcup \mathcal{K}^{(1)} \sqcup \mathcal{K}^{(2)}$
- For all $K \in \mathcal{K}^{(2)}$: $E3^{\mathcal{P}}(K,\cdot)$ invokes a 2-call key derivation function
  - $E3^{\mathcal{P}}(K,x) = \Pi_6^{\mathcal{P}}\big(K \| \mathsf{kd}_1^{\mathcal{P}}(K), x\big)$ for a 2-call KDF $\mathsf{kd}_1^{\mathcal{P}} : \{0,1\}^\kappa \to \{0,1\}^{2m_{max}}$ and a 1-call cipher $\Pi_6^{\mathcal{P}} : \{0,1\}^{\kappa+2m_{max}} \times \{0,1\}^n \to \{0,1\}^n$;
- For all $K \in \mathcal{K}^{(1)}$: $E3^{\mathcal{P}}(K,\cdot)$ invokes a 1-call key derivation function
  - $E3^{\mathcal{P}}(K,x) = \Pi_5^{\mathcal{P}}\big(K \| \mathsf{kd}_2^{\mathcal{P}}(K), \Pi_4^{\mathcal{P}}(K \| \mathsf{kd}_2^{\mathcal{P}}(K), x)\big)$ for a 1-call KDF $\mathsf{kd}_2^{\mathcal{P}} : \{0,1\}^\kappa \to \{0,1\}^{m_{max}}$ and two 1-call ciphers $\Pi_4^{\mathcal{P}}, \Pi_5^{\mathcal{P}} : \{0,1\}^{\kappa+m_{max}} \times \{0,1\}^n \to \{0,1\}^n$;
- For all $K \in \mathcal{K}^{(0)}$: there is no key derivation in the form of oracle procedures
  - $E3^{\mathcal{P}}(K,x) = \Pi_3^{\mathcal{P}}\big(K, \Pi_2^{\mathcal{P}}\big(K, \Pi_1^{\mathcal{P}}(K,x)\big)\big)$ for three 1-call ciphers $\Pi_1^{\mathcal{P}}, \Pi_2^{\mathcal{P}}, \Pi_3^{\mathcal{P}} : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$.

Section 4

Conclusion

Conclusion

The first general lower bounds on indifferentiable blockciphers.

1. (Informal) No iterated blockcipher making 3 or less calls to the oracle $\mathcal{P}$ is statistically indifferentiable from ideal ciphers.
   - The 4-call positive result [GL16] is thus optimal.
2. Model of blockciphers: oracle procedures built upon the oracle $\mathcal{P} = (\mathbf{P}_1, ..., \mathbf{P}_{|\mathcal{I}|})$
3. *Fundamental Properties* of blockciphers oracle procedures
4. Concrete models for 1-call blockciphers $E1^{\mathcal{P}}$ and 2- and 3-call iterated blockciphers $E2^{\mathcal{P}}$ and $E3^{\mathcal{P}}$
5. Attack ideas: using invertibility; using Extremal Graph Theory

Discussion: on blockcipher designs

1. *Expense of overcoming non-invertibility*: inverse-free rounds must admit severe weakness, regardless of its design.
2. *Unhelpfulness of wide permutations*: wide permutations with width$> n$ are not "more helpful" in constructing n-bit blockciphers.
3. *"Excluding-type" theoretical support for popular structures, e.g., the IEM ciphers [DSST17, GL16]*: *no other choice can be better*.
4. An anonymous reviewer: permutation-based cryptography are more efficient than ideal ciphers.

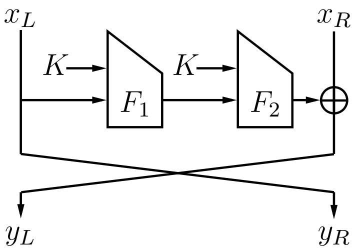
Discussion: on blockcipher designs

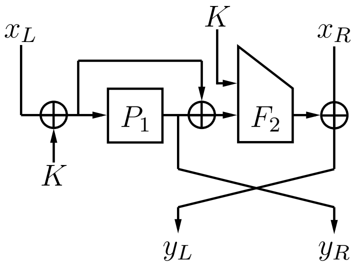
1. *Expense of overcoming non-invertibility*: inverse-free rounds must admit severe weakness, regardless of its design.
2. *Unhelpfulness of wide permutations*: wide permutations with width$> n$ are not "more helpful" in constructing n-bit blockciphers.
3. *"Excluding-type" theoretical support for popular structures, e.g., the IEM ciphers [DSST17, GL16]*: *no other choice can be better*.
4. An anonymous reviewer: permutation-based cryptography are more efficient than ideal ciphers.

- Usual caveats: information-theoretic security upper bounds only

Possible future Directions

1. Extending our treatments to fully general 2- and 3-call blockciphers
   - Blockciphers are *not* necessarily iterated...





Possible future Directions

1. Extending our treatments to fully general 2- and 3-call blockciphers
2. Smart ideas to unify the complicated cases in $E3$ analysis
3. Fully concrete security characterizations of $E2$ and $E3$ (may need a new paradigm)
4. Other aspects: memory restrictions on adversaries/simulators, etc.
5. Achievability of computational indifferentiability with 3 calls
   - Hardness assumptions on graph problems or key derivation functions might be helpful.
6. Relaxing the condition "$Et^{\mathcal{P}}$ computes a blockcipher for all $\mathcal{P}$ and all n"?

Bibliography I

Elena Andreeva, Andrey Bogdanov, Yevgeniy Dodis, Bart Mennink, and John P. Steinberger.
On the indifferentiability of key-alternating ciphers.
In *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 531–550. Springer, 2013.

Paul Baecher, Christina Brzuska, and Arno Mittelbach.
Reset indifferentiability and its consequences.
In *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 154–173. Springer, 2013.

Manuel Barbosa and Pooya Farshim.
Indifferentiable authenticated encryption.
In *CRYPTO 2018, Part I*, volume 10991 of *LNCS*, pages 187–220. Springer, 2018.

Jean-Sébastien Coron, Yevgeniy Dodis, Avradip Mandal, and Yannick Seurin.
A domain extender for the ideal cipher.
In *TCC 2010*, volume 5978 of *LNCS*, pages 273–289. Springer, 2010.

Wonseok Choi, ByeongHak Lee, and Jooyoung Lee.
Indifferentiability of truncated random permutations.
In *ASIACRYPT 2019, Part I*, LNCS, pages 175–195. Springer, 2019.

Jean-Sébastien Coron, Jacques Patarin, and Yannick Seurin.
The random oracle model and the ideal cipher model are equivalent.
In *CRYPTO 2008*, volume 5157 of *LNCS*, pages 1–20. Springer, 2008.

Gregory Demay, Peter Gaži, Martin Hirt, and Ueli Maurer.
Resource-restricted indifferentiability.
In *EUROCRYPT 2013*, LNCS, pages 664–683. Springer, 2013.

Bibliography II

Dana Dachman-Soled, Jonathan Katz, and Aishwarya Thiruvengadam.
10-round Feistel is indifferentiable from an ideal cipher.
In *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 649–678. Springer, 2016.

Yevgeniy Dodis, Thomas Ristenpart, John P. Steinberger, and Stefano Tessaro.
To hash or not to hash again? (In)differentiability results for H^2 and HMAC.
In *CRYPTO 2012*, volume 7417 of *LNCS*, pages 348–366. Springer, 2012.

Yuanxi Dai and John P. Steinberger.
Indifferentiability of 8-round Feistel networks.
In *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 95–120. Springer, 2016.

Yevgeniy Dodis, Martijn Stam, John P. Steinberger, and Tianren Liu.
Indifferentiability of confusion-diffusion networks.
In *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 679–704. Springer, 2016.

Yuanxi Dai, Yannick Seurin, John P. Steinberger, and Aishwarya Thiruvengadam.
Indifferentiability of iterated Even-Mansour ciphers with non-idealized key-schedules: Five rounds are necessary and sufficient.
In *CRYPTO 2017, Part III*, volume 10403 of *LNCS*, pages 524–555. Springer, 2017.

Shimon Even and Yishay Mansour.
A construction of a cipher from a single pseudorandom permutation.
J. Cryptology, 10(3):151–162, June 1997.

Chun Guo and Dongdai Lin.
Indifferentiability of 3-round Even-Mansour with random oracle key derivation.
Cryptology ePrint Archive, Report 2016/894, 2016.
https://eprint.iacr.org/2016/894.

Bibliography III

Chun Guo, Dongdai Lin, and Meicheng Liu.
Cascade ciphers revisited: Indifferentiability analysis.
Cryptology ePrint Archive, Report 2016/825, 2016.
https://eprint.iacr.org/2016/825.

Thomas Holenstein, Robin Künzler, and Stefano Tessaro.
The equivalence of the random oracle model and the ideal cipher model, revisited.
pages 89–98. ACM Press, 2011.

Shlomo Hoory.
The Size of Bipartite Graphs with a Given Girth.
J. Comb. Theory, Ser. B, 86(2):215–220, 2002.

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

Sondre Rønjom, Navid Ghaedi Bardeh, and Tor Helleseth.
Yoyo tricks with AES.
In *ASIACRYPT 2017, Part I*, LNCS, pages 217–243. Springer, 2017.

Thomas Ristenpart, Hovav Shacham, and Thomas Shrimpton.
Careful with composition: Limitations of the indifferentiability framework.
In *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 487–506. Springer, 2011.