Minimizing the Two-Round Even-Mansour Cipher

Shan Chen[1] Rodolphe Lampe[2] Jooyoung Lee[3]
Yannick Seurin[4] John Steinberger[1]

[1]Tsinghua University, China

[2]University of Versailles, France

[3]Sejong University, Korea

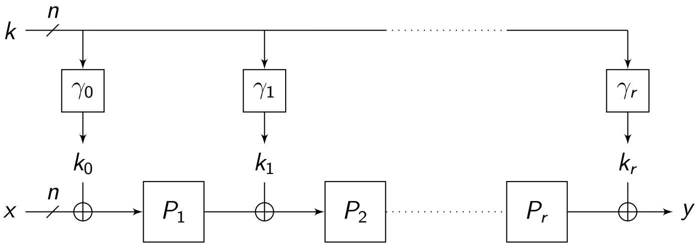
[4]ANSSI, France

August 18, 2014 - CRYPTO 2014

Outline

1. Context: Security Proofs for Key-Alternating Ciphers
2. Overview of our Results
3. Sketch of the Security Proof

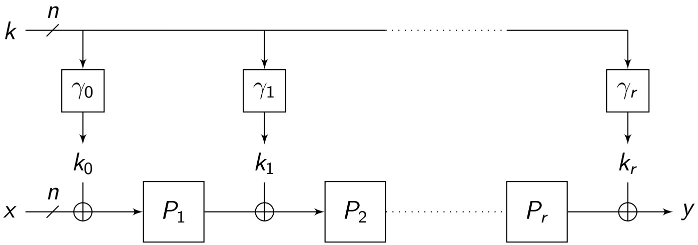
Key-alternating ciphers



An r-round key-alternating cipher

- $k \in \{0,1\}^n$ is the (master) key, x the plaintext, y the ciphertext
- The P_i's are public permutations on $\{0,1\}^n$
- The γ_i's are key derivation functions mapping k to n-bit "round keys"
- prominent example: AES-128

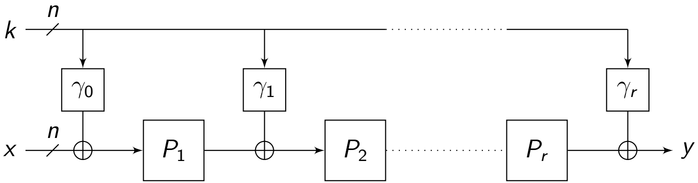
Key-alternating ciphers



An r-round key-alternating cipher

- $k \in \{0,1\}^n$ is the (master) key, x the plaintext, y the ciphertext
- The P_i's are public permutations on $\{0,1\}^n$
- The γ_i's are key derivation functions mapping k to n-bit "round keys"
- prominent example: AES-128

Proving the security of key-alternating ciphers

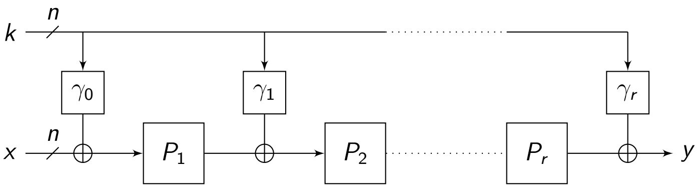


Question

How can we "prove" security? (for this talk, security = pseudorandomness)

- against a general adversary: too hard! (unconditional complexity lower bound)
- against specific attacks (differential, linear...): use specific design of $P_1, \ldots, P_r$, count active S-boxes, etc.
- against generic attacks: Random Permutation Model for $P_1, \ldots, P_r$

Proving the security of key-alternating ciphers

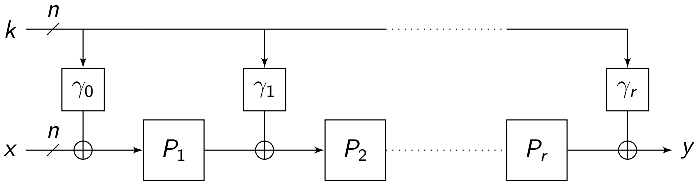


Question

How can we "prove" security? (for this talk, security = pseudorandomness)

- against a general adversary: too hard! (unconditional complexity lower bound)
- against specific attacks (differential, linear...): use specific design of $P_1, \ldots, P_r$, count active S-boxes, etc.
- against generic attacks: Random Permutation Model for $P_1, \ldots, P_r$

Proving the security of key-alternating ciphers

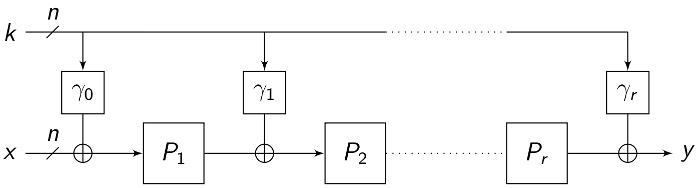


Question

How can we "prove" security? (for this talk, security = pseudorandomness)

- against a general adversary: too hard! (unconditional complexity lower bound)
- against specific attacks (differential, linear...): use specific design of $P_1, \dots, P_r$, count active S-boxes, etc.
- against generic attacks: Random Permutation Model for $P_1, \dots, P_r$

Proving the security of key-alternating ciphers

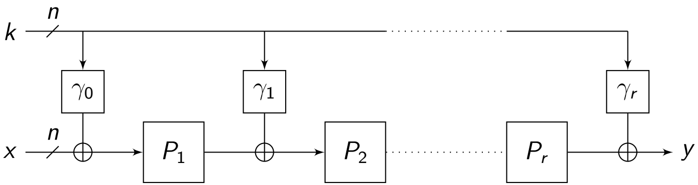


Question

How can we "prove" security? (for this talk, security = pseudorandomness)

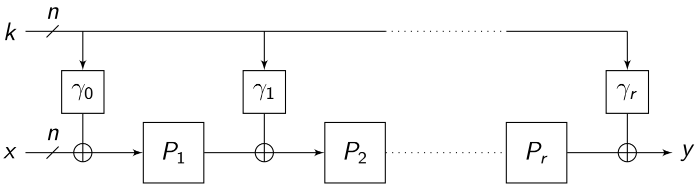
- against a general adversary: too hard! (unconditional complexity lower bound)
- against specific attacks (differential, linear...): use specific design of $P_1, \ldots, P_r$, count active S-boxes, etc.
- against generic attacks: Random Permutation Model for $P_1, \ldots, P_r$

Analyzing KA ciphers in the Random Permutation Model



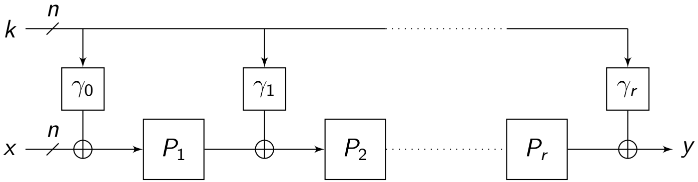
- the P_i's are viewed as public random permutation oracles to which the adversary can only make black-box queries (both to P_i and P_i^{-1}).
- trades complexity for randomness and allows for a completely information-theoretic proof ($\simeq$ Random Oracle Model)
- complexity measure of the adversary:
  - q_e = number of queries to the cipher (plaintext/ciphertext pairs)
  - q_p = number of queries to each internal permutation oracle

Analyzing KA ciphers in the Random Permutation Model



- the P_i's are viewed as public random permutation oracles to which the adversary can only make black-box queries (both to P_i and P_i^{-1}).
- trades complexity for randomness and allows for a completely information-theoretic proof ($\simeq$ Random Oracle Model)
- complexity measure of the adversary:
  - q_e = number of queries to the cipher (plaintext/ciphertext pairs)
  - q_p = number of queries to each internal permutation oracle

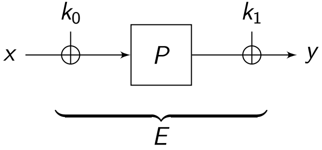
Analyzing KA ciphers in the Random Permutation Model



- the P_i's are viewed as public random permutation oracles to which the adversary can only make black-box queries (both to P_i and P_i^{-1}).
- trades complexity for randomness and allows for a completely information-theoretic proof ($\simeq$ Random Oracle Model)
- complexity measure of the adversary:
  - q_e = number of queries to the cipher (plaintext/ciphertext pairs)
  - q_p = number of queries to each internal permutation oracle

Analyzing KA ciphers in the Random Permutation Model

This model was already considered 15 years ago by Even and Mansour [EM97] for $r = 1$ round: they showed that the following cipher is secure up to $\mathcal{O}(2^{\frac{n}{2}})$ queries of the adversary to P and E:



Similar result when $k_0 = k_1$ [DKS12]

Wording: "(iterated) Even-Mansour cipher" = shorthand for "analyzing the class of key-alternating ciphers in the Random Permutation Model"

Analyzing KA ciphers in the Random Permutation Model

This model was already considered 15 years ago by Even and Mansour [EM97] for $r = 1$ round: they showed that the following cipher is secure up to $\mathcal{O}(2^{\frac{n}{2}})$ queries of the adversary to P and E:

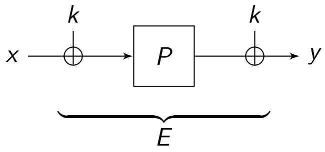
$$\underbrace{x \longrightarrow \oplus k \longrightarrow \boxed{P} \longrightarrow \oplus k \longrightarrow y}_{E}$$

Similar result when $k_0 = k_1$ [DKS12]

Wording: "(iterated) Even-Mansour cipher" = shorthand for "analyzing the class of key-alternating ciphers in the Random Permutation Model"

Analyzing KA ciphers in the Random Permutation Model

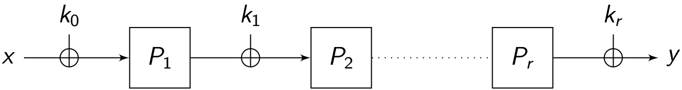
This model was already considered 15 years ago by Even and Mansour [EM97] for $r = 1$ round: they showed that the following cipher is secure up to $\mathcal{O}(2^{\frac{n}{2}})$ queries of the adversary to P and E:



Similar result when $k_0 = k_1$ [DKS12]

Wording: "(iterated) Even-Mansour cipher" = shorthand for "analyzing the class of key-alternating ciphers in the Random Permutation Model"

Outline



Closing a series of recent results [BKL+12, Ste12, LPS12], Chen and Steinberger [CS14] showed that assuming

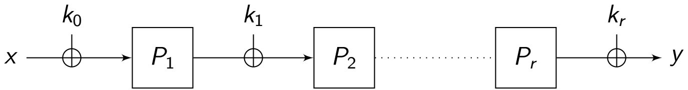
1. independent round keys $(k_0, k_1, \ldots, k_r)$,
2. independent inner permutations $P_1, \ldots, P_r$,

KA ciphers are secure against generic attacks as long as

$$q_e \text{ and } q_p \ll \mathcal{O}(2^{\frac{rn}{r+1}}).$$

This result is tight (in terms of query complexity).

State of the art



Closing a series of recent results [BKL+12, Ste12, LPS12], Chen and Steinberger [CS14] showed that assuming

1. independent round keys $(k_0, k_1, \ldots, k_r)$,
2. independent inner permutations $P_1, \ldots, P_r$,

KA ciphers are secure against generic attacks as long as

$$q_e \text{ and } q_p \ll \mathcal{O}(2^{\frac{rn}{r+1}}).$$

This result is tight (in terms of query complexity).

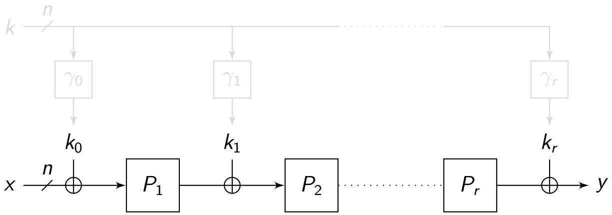
Our problem

Main question

Is it possible to prove a similar $\mathcal{O}(2^{\frac{rn}{r+1}})$ bound when:

- the round keys $(k_0, \ldots, k_r)$ are derived from an n-bit master key
- and/or when the same permutation P is used at each round

as is the case in many concrete designs (AES-128, etc.)?



We give a positive answer for $r = 2$ rounds: $\mathcal{O}(2^{\frac{2n}{3}})$-security bound.

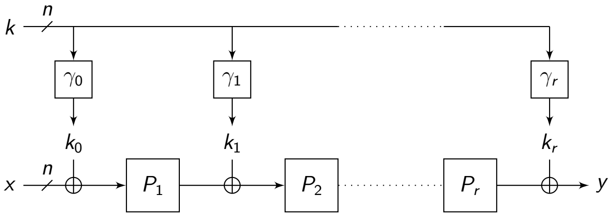
Our problem

Main question

Is it possible to prove a similar $\mathcal{O}(2^{\frac{rn}{r+1}})$ bound when:

- the round keys $(k_0, \ldots, k_r)$ are derived from an n-bit master key
- and/or when the same permutation P is used at each round

as is the case in many concrete designs (AES-128, etc.)?



We give a positive answer for $r = 2$ rounds: $\mathcal{O}(2^{\frac{2n}{3}})$-security bound.

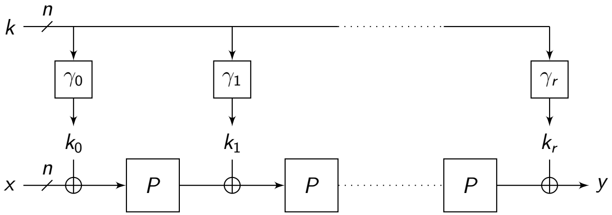
Our problem

Main question

Is it possible to prove a similar $\mathcal{O}(2^{\frac{rn}{r+1}})$ bound when:

- the round keys $(k_0, \ldots, k_r)$ are derived from an n-bit master key
- and/or when the same permutation P is used at each round

as is the case in many concrete designs (AES-128, etc.)?



We give a positive answer for $r = 2$ rounds: $\mathcal{O}(2^{\frac{2n}{3}})$-security bound.

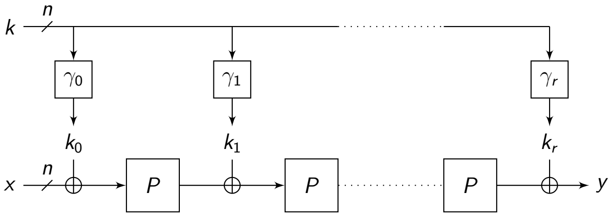
Our problem

Main question

Is it possible to prove a similar $\mathcal{O}(2^{\frac{rn}{r+1}})$ bound when:

- the round keys $(k_0, \ldots, k_r)$ are derived from an n-bit master key
- and/or when the same permutation P is used at each round

as is the case in many concrete designs (AES-128, etc.)?



We give a positive answer for $r = 2$ rounds: $\mathcal{O}(2^{\frac{2n}{3}})$-security bound.

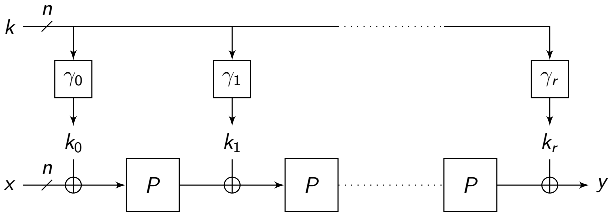
Our problem

Main question

Is it possible to prove a similar $\mathcal{O}(2^{\frac{rn}{r+1}})$ bound when:

- the round keys $(k_0, \ldots, k_r)$ are derived from an n-bit master key
- and/or when the same permutation P is used at each round

as is the case in many concrete designs (AES-128, etc.)?



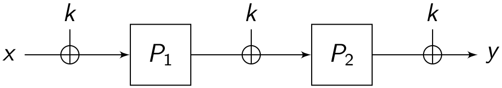
We give a positive answer for $r = 2$ rounds: $\mathcal{O}(2^{\frac{2n}{3}})$-security bound.

Our results (1/2): two independent permutations

First, we deal with the (simpler) case where the two inner permutations are independent. Then the trivial key-schedule is sufficient.

Theorem

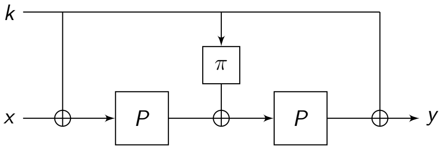
The 2-round EM cipher with independent random permutations and identical round keys is secure up to $\widetilde{\mathcal{O}}(2^{\frac{2n}{3}})$ queries of the adversary.



Our results (2/2): one single permutation

Theorem

The 2-round EM cipher below is secure up to $\widetilde{\mathcal{O}}(2^{\frac{2n}{3}})$ queries of the adversary.



π can be any fixed ($\mathbb{F}_2$-linear) orthomorphism (i.e., π is a permutation and $k \mapsto k \oplus \pi(k)$ is a permutation), for instance

$$\pi : (k_L, k_R) \mapsto (k_R, k_L \oplus k_R) \quad \text{(Feistel)}$$
$$\pi : k \mapsto c \odot k, \quad \text{for } c \neq 0, 1 \quad \text{(field mult.)}$$

Our results (2/2): one single permutation

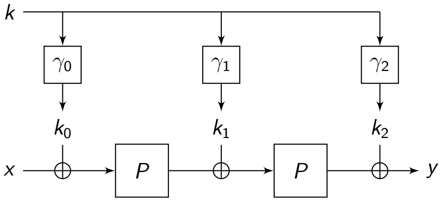
Theorem (more general)

The 2-round EM cipher below is secure up to $\widetilde{\mathcal{O}}(2^{\frac{2n}{3}})$ queries when

(i) $\gamma_0, \gamma_1, \gamma_2$ *are* $\mathbb{F}_2$*-linear permutations;*

(ii) $\gamma_0 \oplus \gamma_1$ *and* $\gamma_1 \oplus \gamma_2$ *are permutations;*

(iii) $\gamma_0 \oplus \gamma_1 \oplus \gamma_2$ *is a permutation.*



Conjecture: $\mathbb{F}_2$-linearity and (*iii*) are not needed.

Our results (2/2): one single permutation

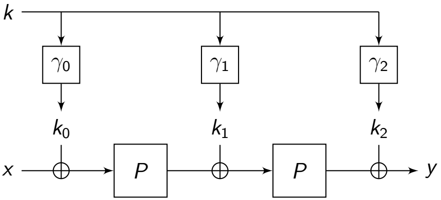
Theorem (more general)

The 2-round EM cipher below is secure up to $\widetilde{\mathcal{O}}(2^{\frac{2n}{3}})$ queries when

(i) $\gamma_0, \gamma_1, \gamma_2$ *are* $\mathbb{F}_2$*-linear permutations;*

(ii) $\gamma_0 \oplus \gamma_1$ *and* $\gamma_1 \oplus \gamma_2$ *are permutations;* *OK for* $(k, \pi(k), k)$

(iii) $\gamma_0 \oplus \gamma_1 \oplus \gamma_2$ *is a permutation.*



Conjecture: $\mathbb{F}_2$-linearity and (*iii*) are not needed.

Our results (2/2): one single permutation

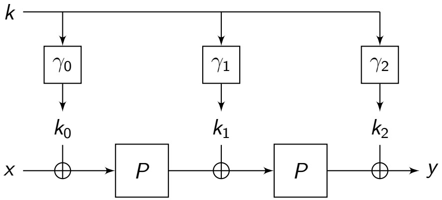
Theorem (more general)

The 2-round EM cipher below is secure up to $\widetilde{\mathcal{O}}(2^{\frac{2n}{3}})$ queries when

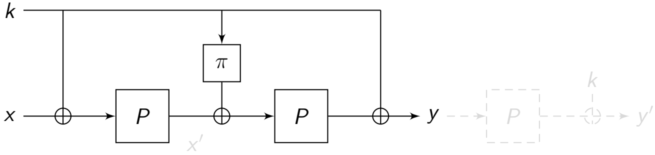
(i) $\gamma_0, \gamma_1, \gamma_2$ *are $\mathbb{F}_2$-linear permutations;*

(ii) $\gamma_0 \oplus \gamma_1$ *and* $\gamma_1 \oplus \gamma_2$ *are permutations;* *OK for $(k, \pi(k), k)$*

(iii) $\gamma_0 \oplus \gamma_1 \oplus \gamma_2$ *is a permutation.*



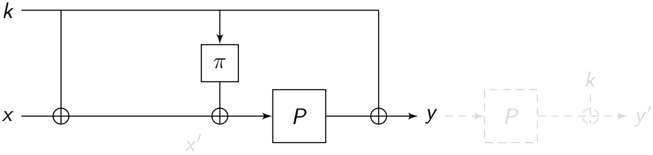
Conjecture: $\mathbb{F}_2$-linearity and (iii) are not needed.



This construction is "minimal" to achieve $\mathcal{O}(2^{\frac{2n}{3}})$ security.
Removing any component causes security to drop back to $\mathcal{O}(2^{\frac{n}{2}})$:

- removing one of the P's: 1-round Even-Mansour, $\mathcal{O}(2^{\frac{n}{2}})$-secure
- removing π: slide attack with $\mathcal{O}(2^{\frac{n}{2}})$ complexity:
  - find $(x, y), (x', y')$ such that $x' = P(x \oplus k)$ (slid pair)
  - can be detected by checking that $x \oplus P(y) = y' \oplus P^{-1}(x')$
  - works for any number of rounds for id. round keys and id. permutations

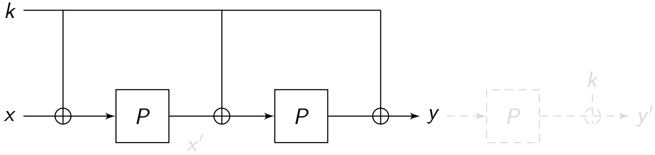
Minimality of the construction



This construction is "minimal" to achieve $\mathcal{O}(2^{\frac{2n}{3}})$ security.
Removing any component causes security to drop back to $\mathcal{O}(2^{\frac{n}{2}})$:

- removing one of the P's: 1-round Even-Mansour, $\mathcal{O}(2^{\frac{n}{2}})$-secure
- removing π: slide attack with $\mathcal{O}(2^{\frac{n}{2}})$ complexity:
  - find $(x, y), (x', y')$ such that $x' = P(x \oplus k)$ (slid pair)
  - can be detected by checking that $x \oplus P(y) = y' \oplus P^{-1}(x')$
  - works for any number of rounds for id. round keys and id. permutations

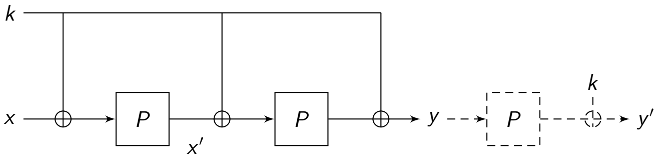
Minimality of the construction



This construction is "minimal" to achieve $\mathcal{O}(2^{\frac{2n}{3}})$ security.
Removing any component causes security to drop back to $\mathcal{O}(2^{\frac{n}{2}})$:

- removing one of the P's: 1-round Even-Mansour, $\mathcal{O}(2^{\frac{n}{2}})$-secure
- removing π: slide attack with $\mathcal{O}(2^{\frac{n}{2}})$ complexity:
  - find $(x, y), (x', y')$ such that $x' = P(x \oplus k)$ (slid pair)
  - can be detected by checking that $x \oplus P(y) = y' \oplus P^{-1}(x')$
  - works for any number of rounds for id. round keys and id. permutations

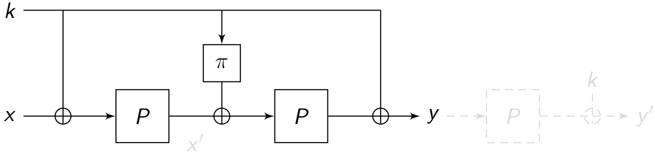
Minimality of the construction



This construction is "minimal" to achieve $\mathcal{O}(2^{\frac{2n}{3}})$ security.
Removing any component causes security to drop back to $\mathcal{O}(2^{\frac{n}{2}})$:

- removing one of the P's: 1-round Even-Mansour, $\mathcal{O}(2^{\frac{n}{2}})$-secure
- removing π: slide attack with $\mathcal{O}(2^{\frac{n}{2}})$ complexity:
  - find $(x, y), (x', y')$ such that $x' = P(x \oplus k)$ (slid pair)
  - can be detected by checking that $x \oplus P(y) = y' \oplus P^{-1}(x')$
  - works for any number of rounds for id. round keys and id. permutations

Minimality of the construction

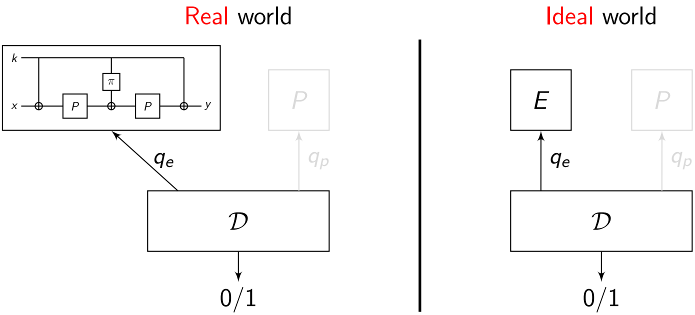


This construction is "minimal" to achieve $\mathcal{O}(2^{\frac{2n}{3}})$ security.
Removing any component causes security to drop back to $\mathcal{O}(2^{\frac{n}{2}})$:

- removing one of the P's: 1-round Even-Mansour, $\mathcal{O}(2^{\frac{n}{2}})$-secure
- removing π: slide attack with $\mathcal{O}(2^{\frac{n}{2}})$ complexity:
  - find $(x, y), (x', y')$ such that $x' = P(x \oplus k)$ (slid pair)
  - can be detected by checking that $x \oplus P(y) = y' \oplus P^{-1}(x')$
  - works for any number of rounds for id. round keys and id. permutations

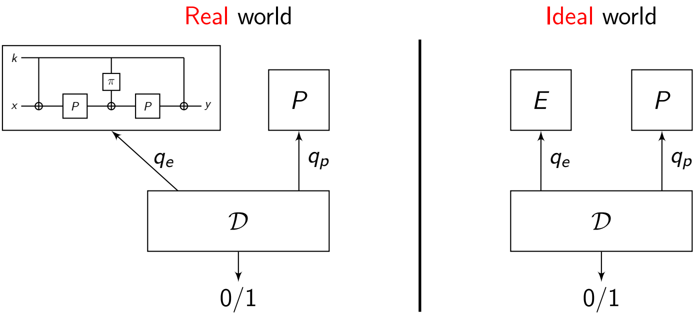
Outline

Formalizing indistinguishability (in the RP Model)



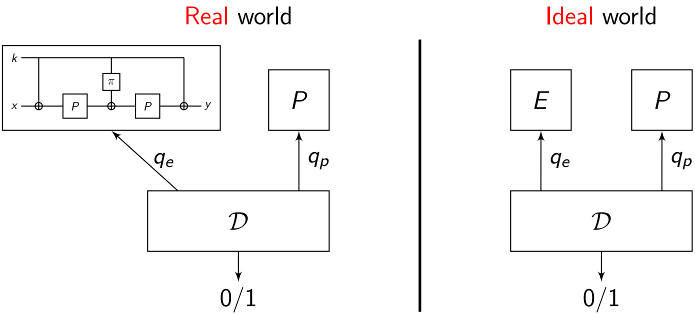
- real world: cipher with a random key $k \leftarrow_{\$} \{0,1\}^n$
- ideal world: E is a random permutation independent from P
- Random Permutation Model: $\mathcal{D}$ has oracle access to P in both worlds
- for this talk, $q_e = q_p = q$

Formalizing indistinguishability (in the RP Model)



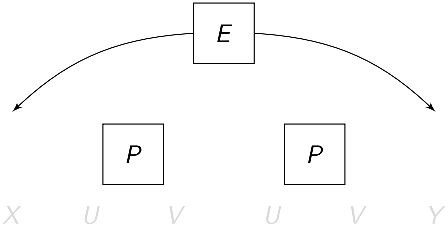
- real world: cipher with a random key $k \leftarrow_{\$} \{0,1\}^n$
- ideal world: E is a random permutation independent from P
- Random Permutation Model: $\mathcal{D}$ has oracle access to P in both worlds
- for this talk, $q_e = q_p = q$

Formalizing indistinguishability (in the RP Model)



- real world: cipher with a random key $k \leftarrow_{\$} \{0,1\}^n$
- ideal world: E is a random permutation independent from P
- Random Permutation Model: $\mathcal{D}$ has oracle access to P in both worlds
- for this talk, $q_e = q_p = q$

Query transcript



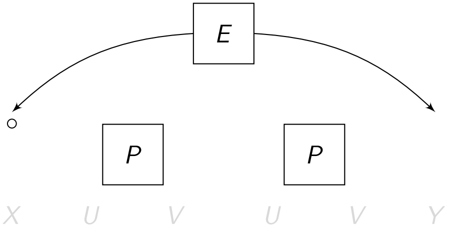
The distinguisher can query:

- oracle E forward: $E(x) = y$, and backward: $E^{-1}(y) = x$
- oracle P forward: $P(u) = v$, and backward: $P^{-1}(v) = u$

This results in a query transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$:

$$\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$$
$$\mathcal{Q}_P = \{(u_1, v_1), \ldots, (u_q, v_q)\}.$$

Query transcript



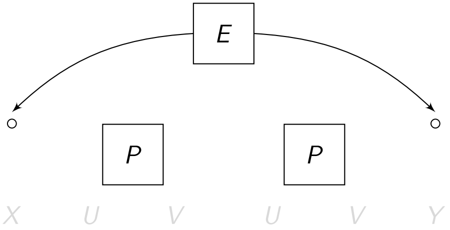
The distinguisher can query:

- oracle E forward: $E(x) = y$, and backward: $E^{-1}(y) = x$
- oracle P forward: $P(u) = v$, and backward: $P^{-1}(v) = u$

This results in a query transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$:

$$\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$$
$$\mathcal{Q}_P = \{(u_1, v_1), \ldots, (u_q, v_q)\}.$$

Query transcript



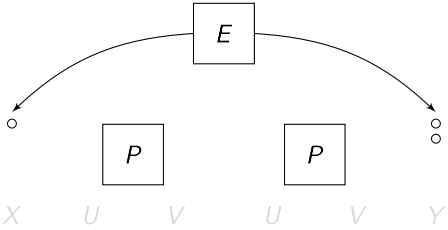
The distinguisher can query:

- oracle E forward: $E(x) = y$, and backward: $E^{-1}(y) = x$
- oracle P forward: $P(u) = v$, and backward: $P^{-1}(v) = u$

This results in a query transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$:

$$\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$$
$$\mathcal{Q}_P = \{(u_1, v_1), \ldots, (u_q, v_q)\}.$$

Query transcript



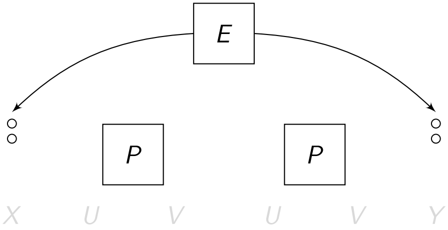
The distinguisher can query:

- oracle E forward: $E(x) = y$, and backward: $E^{-1}(y) = x$
- oracle P forward: $P(u) = v$, and backward: $P^{-1}(v) = u$

This results in a query transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$:

$$\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$$
$$\mathcal{Q}_P = \{(u_1, v_1), \ldots, (u_q, v_q)\}.$$

Query transcript



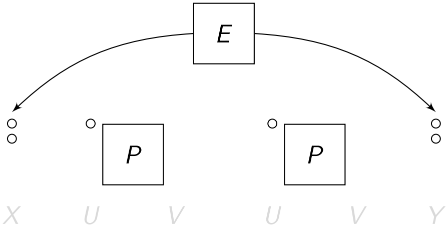
The distinguisher can query:

- oracle E forward: $E(x) = y$, and backward: $E^{-1}(y) = x$
- oracle P forward: $P(u) = v$, and backward: $P^{-1}(v) = u$

This results in a query transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$:

$$\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$$
$$\mathcal{Q}_P = \{(u_1, v_1), \ldots, (u_q, v_q)\}.$$

Query transcript



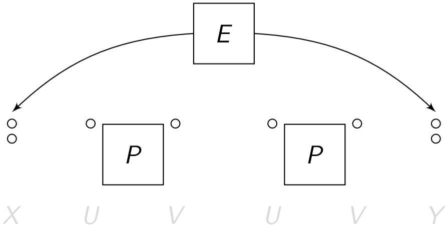
The distinguisher can query:

- oracle E forward: $E(x) = y$, and backward: $E^{-1}(y) = x$
- oracle P forward: $P(u) = v$, and backward: $P^{-1}(v) = u$

This results in a query transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$:

$$\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$$
$$\mathcal{Q}_P = \{(u_1, v_1), \ldots, (u_q, v_q)\}.$$

Query transcript



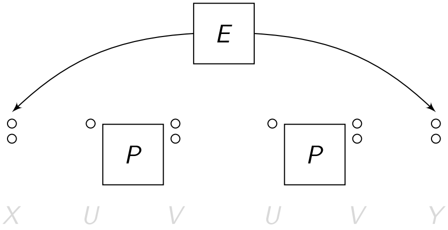
The distinguisher can query:

- oracle E forward: $E(x) = y$, and backward: $E^{-1}(y) = x$
- oracle P forward: $P(u) = v$, and backward: $P^{-1}(v) = u$

This results in a query transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$:

$$\mathcal{Q}_E = \{(x_1, y_1), \dots, (x_q, y_q)\}$$
$$\mathcal{Q}_P = \{(u_1, v_1), \dots, (u_q, v_q)\}.$$

Query transcript



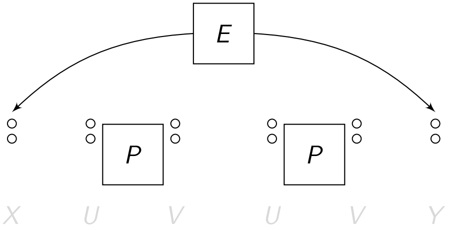
The distinguisher can query:

- oracle E forward: $E(x) = y$, and backward: $E^{-1}(y) = x$
- oracle P forward: $P(u) = v$, and backward: $P^{-1}(v) = u$

This results in a query transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$:

$$\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$$
$$\mathcal{Q}_P = \{(u_1, v_1), \ldots, (u_q, v_q)\}.$$

Query transcript



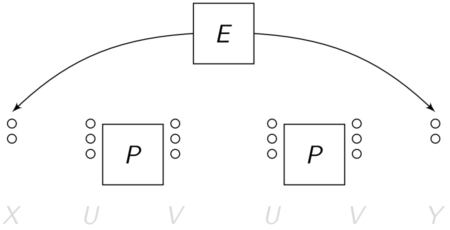
The distinguisher can query:

- oracle E forward: $E(x) = y$, and backward: $E^{-1}(y) = x$
- oracle P forward: $P(u) = v$, and backward: $P^{-1}(v) = u$

This results in a query transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$:

$$\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$$
$$\mathcal{Q}_P = \{(u_1, v_1), \ldots, (u_q, v_q)\}.$$

Query transcript



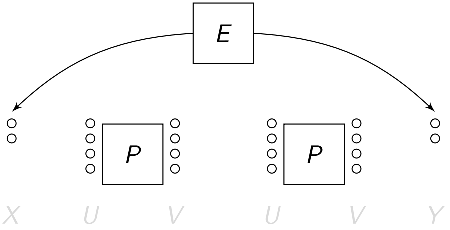
The distinguisher can query:

- oracle E forward: $E(x) = y$, and backward: $E^{-1}(y) = x$
- oracle P forward: $P(u) = v$, and backward: $P^{-1}(v) = u$

This results in a query transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$:

$$\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$$
$$\mathcal{Q}_P = \{(u_1, v_1), \ldots, (u_q, v_q)\}.$$

Query transcript



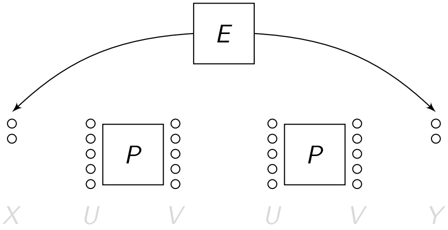
The distinguisher can query:

- oracle E forward: $E(x) = y$, and backward: $E^{-1}(y) = x$
- oracle P forward: $P(u) = v$, and backward: $P^{-1}(v) = u$

This results in a query transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$:

$$\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$$
$$\mathcal{Q}_P = \{(u_1, v_1), \ldots, (u_q, v_q)\}.$$

Query transcript



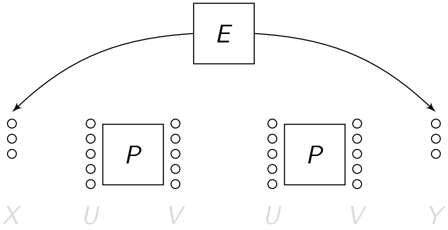
The distinguisher can query:

- oracle E forward: $E(x) = y$, and backward: $E^{-1}(y) = x$
- oracle P forward: $P(u) = v$, and backward: $P^{-1}(v) = u$

This results in a query transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$:

$$\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$$
$$\mathcal{Q}_P = \{(u_1, v_1), \ldots, (u_q, v_q)\}.$$

Query transcript



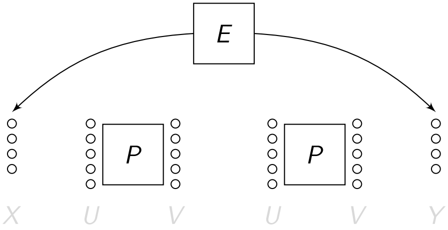
The distinguisher can query:

- oracle E forward: $E(x) = y$, and backward: $E^{-1}(y) = x$
- oracle P forward: $P(u) = v$, and backward: $P^{-1}(v) = u$

This results in a query transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$:

$$\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$$
$$\mathcal{Q}_P = \{(u_1, v_1), \ldots, (u_q, v_q)\}.$$

Query transcript



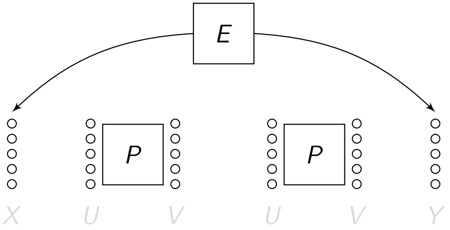
The distinguisher can query:

- oracle E forward: $E(x) = y$, and backward: $E^{-1}(y) = x$
- oracle P forward: $P(u) = v$, and backward: $P^{-1}(v) = u$

This results in a query transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$:

$$\mathcal{Q}_E = \{(x_1, y_1), \dots, (x_q, y_q)\}$$
$$\mathcal{Q}_P = \{(u_1, v_1), \dots, (u_q, v_q)\}.$$

Query transcript



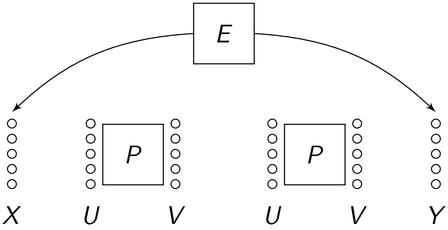
The distinguisher can query:

- oracle E forward: $E(x) = y$, and backward: $E^{-1}(y) = x$
- oracle P forward: $P(u) = v$, and backward: $P^{-1}(v) = u$

This results in a query transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$:

$$\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$$
$$\mathcal{Q}_P = \{(u_1, v_1), \ldots, (u_q, v_q)\}.$$

Query transcript



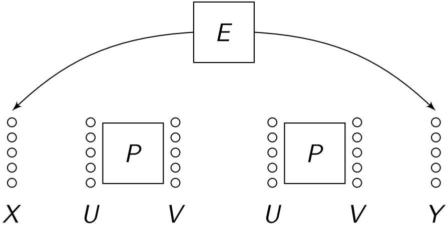
The distinguisher can query:

- oracle E forward: $E(x) = y$, and backward: $E^{-1}(y) = x$
- oracle P forward: $P(u) = v$, and backward: $P^{-1}(v) = u$

This results in a query transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$:

$$\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$$
$$\mathcal{Q}_P = \{(u_1, v_1), \ldots, (u_q, v_q)\}.$$

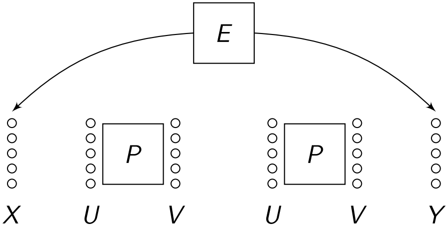
H-coefficient framework



$$\mathbf{Adv}(\mathcal{D}) \leq \| T_{\mathrm{real}} - T_{\mathrm{ideal}} \| \quad \text{(statistical distance)}$$

$$T_{\mathrm{real/ideal}} = \text{distribution of transcript } (\mathcal{Q}_E, \mathcal{Q}_P)$$
$$\text{in the real/ideal world}$$

H-coefficient framework

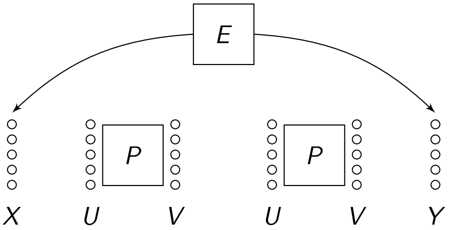


Lemma

Partition the set of transcripts into "good" ones $\mathcal{T}_{\text{good}}$ and "bad" ones $\mathcal{T}_{\text{bad}}$. Then

$$\left.\begin{array}{l} \forall \tau \in \mathcal{T}_{\text{good}}, \frac{\Pr[T_{\text{real}}=\tau]}{\Pr[T_{\text{ideal}}=\tau]} \geq 1-\varepsilon_1 \\ \\ \Pr[T_{\text{ideal}} \in \mathcal{T}_{\text{bad}}] \leq \varepsilon_2 \end{array}\right\} \Rightarrow \mathbf{Adv}(\mathcal{D}) \leq \varepsilon_1 + \varepsilon_2$$

Bad keys and bad transcripts (simplified)



A key k' is bad if $\mathcal{D}$ can check its "compatibility" with the transcript:

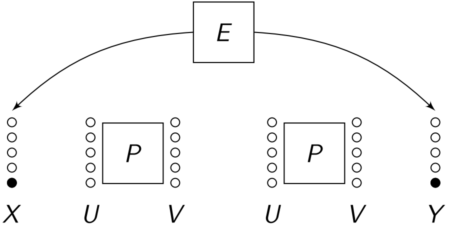
1. $\exists(x, y) \in \mathcal{Q}_E$, $u \in U$, $v \in V$: $k' = x \oplus u = y \oplus v$
2. $\exists(u, v) \in \mathcal{Q}_P$, $x \in X$, $u' \in U$: $k' = x \oplus u$ and $\pi(k') = v \oplus u'$
3. $\exists(u, v) \in \mathcal{Q}_P$, $y \in Y$, $v' \in V$: $k' = v \oplus y$ and $\pi(k') = v' \oplus u$

A transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$ is bad if it has too many bad keys.

We must show that with high probability,

$$\# \text{ bad keys} \ll 2^n.$$

Bad keys and bad transcripts (simplified)



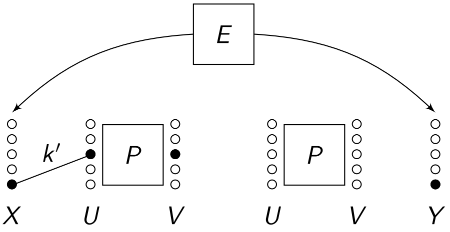
A key k' is bad if $\mathcal{D}$ can check its "compatibility" with the transcript:

1. $\exists (x, y) \in \mathcal{Q}_E,\ u \in U,\ v \in V\colon\ k' = x \oplus u = y \oplus v$
2. $\exists (u, v) \in \mathcal{Q}_P,\ x \in X,\ u' \in U\colon\ k' = x \oplus u$ and $\pi(k') = v \oplus u'$
3. $\exists (u, v) \in \mathcal{Q}_P,\ y \in Y,\ v' \in V\colon\ k' = v \oplus y$ and $\pi(k') = v' \oplus u$

A transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$ is bad if it has too many bad keys.
We must show that with high probability,

$$\#\ \text{bad keys} \ll 2^n.$$

Bad keys and bad transcripts (simplified)



A key k' is bad if $\mathcal{D}$ can check its "compatibility" with the transcript:

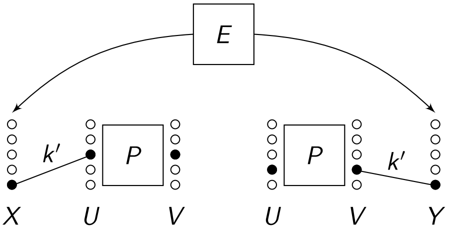
1. $\exists(x, y) \in \mathcal{Q}_E$, $u \in U$, $v \in V$: $k' = x \oplus u = y \oplus v$
2. $\exists(u, v) \in \mathcal{Q}_P$, $x \in X$, $u' \in U$: $k' = x \oplus u$ and $\pi(k') = v \oplus u'$
3. $\exists(u, v) \in \mathcal{Q}_P$, $y \in Y$, $v' \in V$: $k' = v \oplus y$ and $\pi(k') = v' \oplus u$

A transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$ is bad if it has too many bad keys.

We must show that with high probability,

$$\# \text{ bad keys} \ll 2^n.$$

Bad keys and bad transcripts (simplified)



A key k' is bad if $\mathcal{D}$ can check its "compatibility" with the transcript:

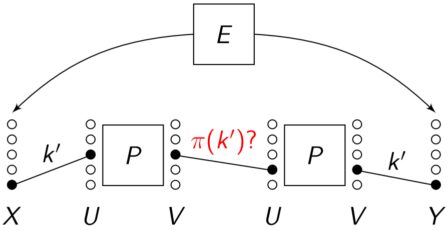
1. $\exists (x, y) \in \mathcal{Q}_E,\ u \in U,\ v \in V$: $k' = x \oplus u = y \oplus v$
2. $\exists (u, v) \in \mathcal{Q}_P,\ x \in X,\ u' \in U$: $k' = x \oplus u$ and $\pi(k') = v \oplus u'$
3. $\exists (u, v) \in \mathcal{Q}_P,\ y \in Y,\ v' \in V$: $k' = v \oplus y$ and $\pi(k') = v' \oplus u$

A transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$ is bad if it has too many bad keys.

We must show that with high probability,

$$\#\ \text{bad keys} \ll 2^n.$$

Bad keys and bad transcripts (simplified)



A key k' is bad if $\mathcal{D}$ can check its "compatibility" with the transcript:

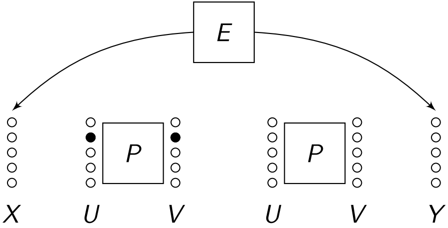
1. $\exists (x, y) \in \mathcal{Q}_E$, $u \in U$, $v \in V$: $k' = x \oplus u = y \oplus v$
2. $\exists (u, v) \in \mathcal{Q}_P$, $x \in X$, $u' \in U$: $k' = x \oplus u$ and $\pi(k') = v \oplus u'$
3. $\exists (u, v) \in \mathcal{Q}_P$, $y \in Y$, $v' \in V$: $k' = v \oplus y$ and $\pi(k') = v' \oplus u$

A transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$ is bad if it has too many bad keys.

We must show that with high probability,

$$\#\text{ bad keys} \ll 2^n.$$

Bad keys and bad transcripts (simplified)



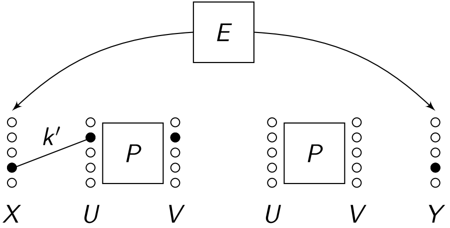
A key k' is bad if $\mathcal{D}$ can check its "compatibility" with the transcript:

1. $\exists (x, y) \in \mathcal{Q}_E$, $u \in U$, $v \in V$: $k' = x \oplus u = y \oplus v$
2. $\exists (u, v) \in \mathcal{Q}_P$, $x \in X$, $u' \in U$: $k' = x \oplus u$ and $\pi(k') = v \oplus u'$
3. $\exists (u, v) \in \mathcal{Q}_P$, $y \in Y$, $v' \in V$: $k' = v \oplus y$ and $\pi(k') = v' \oplus u$

A transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$ is bad if it has too many bad keys.
We must show that with high probability,

$$\#\text{ bad keys} \ll 2^n.$$

Bad keys and bad transcripts (simplified)



A key k' is bad if $\mathcal{D}$ can check its “compatibility” with the transcript:

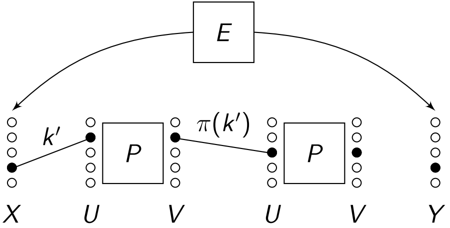
1. $\exists (x, y) \in \mathcal{Q}_E$, $u \in U$, $v \in V$: $k' = x \oplus u = y \oplus v$
2. $\exists (u, v) \in \mathcal{Q}_P$, $x \in X$, $u' \in U$: $k' = x \oplus u$ and $\pi(k') = v \oplus u'$
3. $\exists (u, v) \in \mathcal{Q}_P$, $y \in Y$, $v' \in V$: $k' = v \oplus y$ and $\pi(k') = v' \oplus u$

A transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$ is bad if it has too many bad keys.

We must show that with high probability,

$$\# \text{ bad keys} \ll 2^n.$$

Bad keys and bad transcripts (simplified)



A key k' is bad if $\mathcal{D}$ can check its "compatibility" with the transcript:

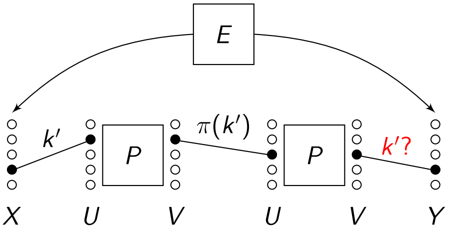
1. $\exists (x, y) \in \mathcal{Q}_E$, $u \in U$, $v \in V$: $k' = x \oplus u = y \oplus v$
2. $\exists (u, v) \in \mathcal{Q}_P$, $x \in X$, $u' \in U$: $k' = x \oplus u$ and $\pi(k') = v \oplus u'$
3. $\exists (u, v) \in \mathcal{Q}_P$, $y \in Y$, $v' \in V$: $k' = v \oplus y$ and $\pi(k') = v' \oplus u$

A transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$ is bad if it has too many bad keys.

We must show that with high probability,

$$\# \text{ bad keys} \ll 2^n.$$

Bad keys and bad transcripts (simplified)



A key k' is bad if $\mathcal{D}$ can check its "compatibility" with the transcript:

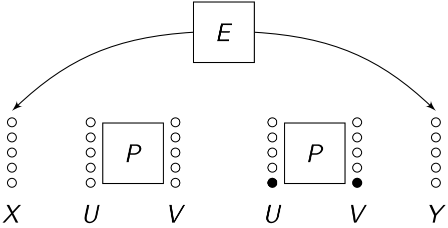
1. $\exists (x, y) \in \mathcal{Q}_E$, $u \in U$, $v \in V$: $k' = x \oplus u = y \oplus v$
2. $\exists (u, v) \in \mathcal{Q}_P$, $x \in X$, $u' \in U$: $k' = x \oplus u$ and $\pi(k') = v \oplus u'$
3. $\exists (u, v) \in \mathcal{Q}_P$, $y \in Y$, $v' \in V$: $k' = v \oplus y$ and $\pi(k') = v' \oplus u$

A transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$ is bad if it has too many bad keys.

We must show that with high probability,

$$\# \text{ bad keys} \ll 2^n.$$

Bad keys and bad transcripts (simplified)



A key k' is bad if $\mathcal{D}$ can check its "compatibility" with the transcript:

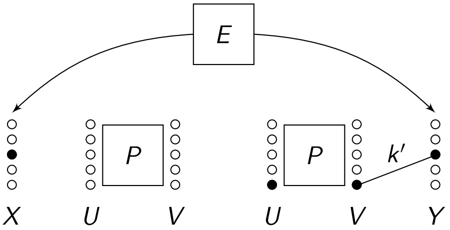
1. $\exists (x, y) \in \mathcal{Q}_E,\ u \in U,\ v \in V$: $k' = x \oplus u = y \oplus v$
2. $\exists (u, v) \in \mathcal{Q}_P,\ x \in X,\ u' \in U$: $k' = x \oplus u$ and $\pi(k') = v \oplus u'$
3. $\exists (u, v) \in \mathcal{Q}_P,\ y \in Y,\ v' \in V$: $k' = v \oplus y$ and $\pi(k') = v' \oplus u$

A transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$ is bad if it has too many bad keys.

We must show that with high probability,

$$\# \text{ bad keys} \ll 2^n.$$

Bad keys and bad transcripts (simplified)



A key k' is bad if $\mathcal{D}$ can check its "compatibility" with the transcript:

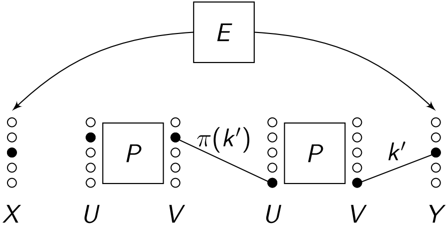
1. $\exists (x, y) \in \mathcal{Q}_E,\ u \in U,\ v \in V$: $k' = x \oplus u = y \oplus v$
2. $\exists (u, v) \in \mathcal{Q}_P,\ x \in X,\ u' \in U$: $k' = x \oplus u$ and $\pi(k') = v \oplus u'$
3. $\exists (u, v) \in \mathcal{Q}_P,\ y \in Y,\ v' \in V$: $k' = v \oplus y$ and $\pi(k') = v' \oplus u$

A transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$ is bad if it has too many bad keys.

We must show that with high probability,

$$\#\ \text{bad keys} \ll 2^n.$$

Bad keys and bad transcripts (simplified)



A key k' is bad if $\mathcal{D}$ can check its "compatibility" with the transcript:

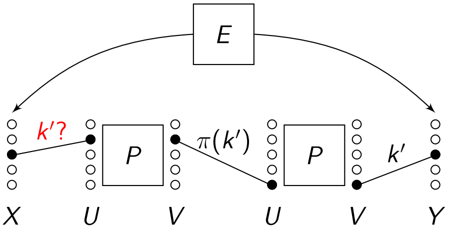
1. $\exists(x,y) \in \mathcal{Q}_E$, $u \in U$, $v \in V$: $k' = x \oplus u = y \oplus v$
2. $\exists(u,v) \in \mathcal{Q}_P$, $x \in X$, $u' \in U$: $k' = x \oplus u$ and $\pi(k') = v \oplus u'$
3. $\exists(u,v) \in \mathcal{Q}_P$, $y \in Y$, $v' \in V$: $k' = v \oplus y$ and $\pi(k') = v' \oplus u$

A transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$ is bad if it has too many bad keys.

We must show that with high probability,

$$\# \text{ bad keys} \ll 2^n.$$

Bad keys and bad transcripts (simplified)



A key k' is bad if $\mathcal{D}$ can check its "compatibility" with the transcript:

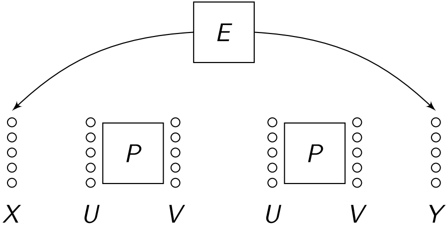
1. $\exists (x, y) \in \mathcal{Q}_E,\ u \in U,\ v \in V\colon\ k' = x \oplus u = y \oplus v$
2. $\exists (u, v) \in \mathcal{Q}_P,\ x \in X,\ u' \in U\colon\ k' = x \oplus u$ and $\pi(k') = v \oplus u'$
3. $\exists (u, v) \in \mathcal{Q}_P,\ y \in Y,\ v' \in V\colon\ k' = v \oplus y$ and $\pi(k') = v' \oplus u$

A transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$ is bad if it has too many bad keys.

We must show that with high probability,

$$\#\text{ bad keys} \ll 2^n.$$

Bad keys and bad transcripts (simplified)



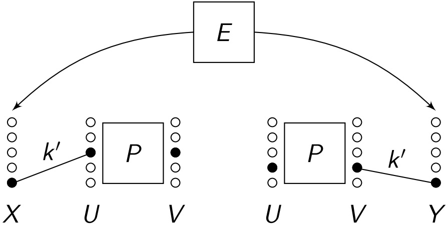
A key k' is bad if $\mathcal{D}$ can check its "compatibility" with the transcript:

1. $\exists(x,y) \in \mathcal{Q}_E$, $u \in U$, $v \in V$: $k' = x \oplus u = y \oplus v$
2. $\exists(u,v) \in \mathcal{Q}_P$, $x \in X$, $u' \in U$: $k' = x \oplus u$ and $\pi(k') = v \oplus u'$
3. $\exists(u,v) \in \mathcal{Q}_P$, $y \in Y$, $v' \in V$: $k' = v \oplus y$ and $\pi(k') = v' \oplus u$

A transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$ is bad if it has too many bad keys.

We must show that with high probability,

$$\#\text{ bad keys} \ll 2^n.$$



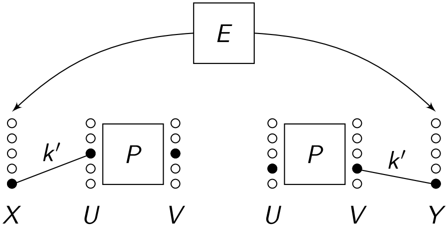
Focus on case 1:

$$\exists (x,y) \in \mathcal{Q}_E,\ u \in U,\ v \in V\colon\ k' = x \oplus u = y \oplus v$$

Then

$$\#\text{ bad keys} \leq \#\{((x,y),u,v) \in \mathcal{Q}_E \times U \times V :\ \underbrace{x \oplus y}_{\simeq\ \text{random}} = u \oplus v\}$$

Upper bounding the number of bad keys



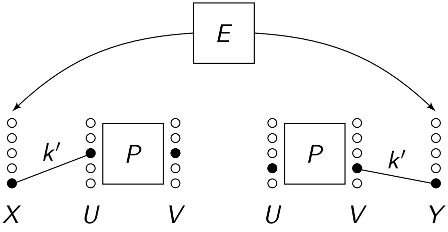
Focus on case 1:

$$\exists (x, y) \in \mathcal{Q}_E,\ u \in U,\ v \in V\colon\ k' = x \oplus u = y \oplus v$$

Then

$$\#\text{ bad keys} \leq \#\{((x,y),u,v) \in \mathcal{Q}_E \times U \times V : \underbrace{x \oplus y}_{\simeq\ \text{random}} = u \oplus v\}$$

Upper bounding the number of bad keys



Focus on case 1:

$$\exists (x,y) \in \mathcal{Q}_E,\ u \in U,\ v \in V\colon\ k' = x \oplus u = y \oplus v$$

Then

$$\#\ \text{bad keys} \leq \#\{((x,y),u,v) \in \mathcal{Q}_E \times U \times V : \underbrace{x \oplus y}_{\simeq\ \textcolor{red}{\text{random}}} = u \oplus v\}$$

The sum-capture problem

For $A = \{a_1, \ldots, a_q\} \subseteq \{0,1\}^n$, let

$$\mu(A) = \max_{\substack{U,V \subseteq \{0,1\}^n \\ |U|=|V|=q}} |\{(a,u,v) \in A \times U \times V : a = u \oplus v\}|$$

If A is "structured", e.g. a vector space, then $\mu(A) = q^2$

Sum-capture problem: find upper bounds on $\mu(A)$ for a random set A

Theorem ([Bab89, Ste13])

For $q \leq 2^{\frac{2n}{3}}$, then with overwhelming probability for a random set A,

$$\mu(A) \lesssim q^{\frac{3}{2}}.$$

(Hence $\mu(A) \ll 2^n$ when $q \ll 2^{\frac{2n}{3}}$.)

The sum-capture problem

For $A = \{a_1, \ldots, a_q\} \subseteq \{0,1\}^n$, let

$$\mu(A) = \max_{\substack{U,V \subseteq \{0,1\}^n \\ |U|=|V|=q}} |\{(a,u,v) \in A \times U \times V : a = u \oplus v\}|$$

If A is "structured", e.g. a vector space, then $\mu(A) = q^2$

Sum-capture problem: find upper bounds on $\mu(A)$ for a random set A

Theorem ([Bab89, Ste13])

For $q \leq 2^{\frac{2n}{3}}$, then with overwhelming probability for a random set A,

$$\mu(A) \lesssim q^{\frac{3}{2}}.$$

(Hence $\mu(A) \ll 2^n$ when $q \ll 2^{\frac{2n}{3}}$.)

The sum-capture problem

For $A = \{a_1, \ldots, a_q\} \subseteq \{0,1\}^n$, let

$$\mu(A) = \max_{\substack{U,V \subseteq \{0,1\}^n \\ |U|=|V|=q}} |\{(a,u,v) \in A \times U \times V : a = u \oplus v\}|$$

If A is "structured", e.g. a vector space, then $\mu(A) = q^2$

Sum-capture problem: find upper bounds on $\mu(A)$ for a random set A

Theorem ([Bab89, Ste13])

For $q \leq 2^{\frac{2n}{3}}$, then with overwhelming probability for a random set A,

$$\mu(A) \lesssim q^{\frac{3}{2}}.$$

(Hence $\mu(A) \ll 2^n$ when $q \ll 2^{\frac{2n}{3}}$.)

A new sum-capture theorem

In our case, we need to adapt the theorem to the case where

$$A = \{x_1 \oplus y_1, \ldots, x_q \oplus y_q\} \simeq \text{ random}$$

Theorem

Let $\mathcal{D}$ be an adversary interacting with a random permutation E of $\{0,1\}^n$, resulting in a query transcript $\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$. Let

$$\mu(\mathcal{Q}_E) = \max_{\substack{U,V \subseteq \{0,1\}^n \\ |U|=|V|=q}} |\{((x,y),u,v) \in \mathcal{Q}_E \times U \times V : x \oplus y = u \oplus v\}|$$

If $q \leq 2^{\frac{2n}{3}}$, then with overwhelming probability,

$$\# \text{ bad keys} \leq \mu(\mathcal{Q}_E) \leq 3(\sqrt{n}+1)q^{\frac{3}{2}}.$$

Proof: Fourier analysis.

A new sum-capture theorem

In our case, we need to adapt the theorem to the case where

$$A = \{x_1 \oplus y_1, \ldots, x_q \oplus y_q\} \simeq \text{ random}$$

Theorem

Let $\mathcal{D}$ be an adversary interacting with a random permutation E of $\{0,1\}^n$, resulting in a query transcript $\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$. Let

$$\mu(\mathcal{Q}_E) = \max_{\substack{U,V \subseteq \{0,1\}^n \\ |U|=|V|=q}} |\{((x,y),u,v) \in \mathcal{Q}_E \times U \times V : x \oplus y = u \oplus v\}|$$

If $q \leq 2^{\frac{2n}{3}}$, then with overwhelming probability,

$$\# \text{ bad keys} \leq \mu(\mathcal{Q}_E) \leq 3(\sqrt{n}+1)q^{\frac{3}{2}}.$$

Proof: Fourier analysis.

A new sum-capture theorem

In our case, we need to adapt the theorem to the case where

$$A = \{x_1 \oplus y_1, \ldots, x_q \oplus y_q\} \simeq \text{ random}$$

Theorem

Let $\mathcal{D}$ be an adversary interacting with a random permutation E of $\{0,1\}^n$, resulting in a query transcript $\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$. Let

$$\mu(\mathcal{Q}_E) = \max_{\substack{U,V \subseteq \{0,1\}^n \\ |U|=|V|=q}} |\{((x,y),u,v) \in \mathcal{Q}_E \times U \times V : x \oplus y = u \oplus v\}|$$

If $q \leq 2^{\frac{2n}{3}}$, then with overwhelming probability,

$$\# \text{ bad keys} \leq \mu(\mathcal{Q}_E) \leq 3(\sqrt{n}+1)q^{\frac{3}{2}}.$$

Proof: Fourier analysis.

Good transcripts

For a "good" transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$ with the expected number of bad keys, we are reduced to the following permutation counting problem.

Permutation counting problem (simplified)

Let $X = \{x_1, \ldots, x_q\}$ and $Y = \{y_1, \ldots, y_q\}$ with $X \cap Y$ "small". Compare

$$p_{\text{real}} = \Pr[P \leftarrow_\$ \mathcal{P}_n : P \circ P(x_i) = y_i \text{ for } i = 1, \ldots, q]$$

$$\text{and } p_{\text{ideal}} = \frac{1}{2^n(2^n-1)\cdots(2^n-q+1)} \quad (\Pr[E(x_i) = y_i])$$

Lemma

Assume $|X \cap Y| \leq q/2^{n/3}$. Then $p_{\text{real}} \geq (1 - \varepsilon_1)\, p_{\text{ideal}}$ with $\varepsilon_1 = \mathcal{O}\left(\frac{q^3}{2^{2n}}\right)$.

Proof: intricate counting ☹

Good transcripts

For a "good" transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P)$ with the expected number of bad keys, we are reduced to the following permutation counting problem.

Permutation counting problem (simplified)

Let $X = \{x_1, \ldots, x_q\}$ and $Y = \{y_1, \ldots, y_q\}$ with $X \cap Y$ "small". Compare

$$p_{\mathrm{real}} = \Pr[P \leftarrow_{\$} \mathcal{P}_n : P \circ P(x_i) = y_i \text{ for } i = 1, \ldots, q]$$

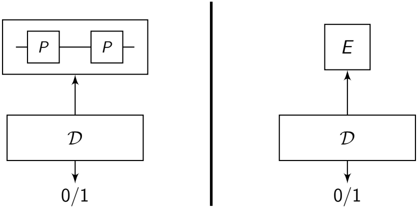
$$\text{and } p_{\mathrm{ideal}} = \frac{1}{2^n(2^n-1)\cdots(2^n-q+1)} \quad (\Pr[E(x_i) = y_i])$$

Lemma

Assume $|X \cap Y| \leq q/2^{n/3}$. *Then* $p_{\mathrm{real}} \geq (1-\varepsilon_1)\, p_{\mathrm{ideal}}$ *with* $\varepsilon_1 = \mathcal{O}\left(\frac{q^3}{2^{2n}}\right)$.

Proof: intricate counting ☹

Random *square* permutation vs. random permutation



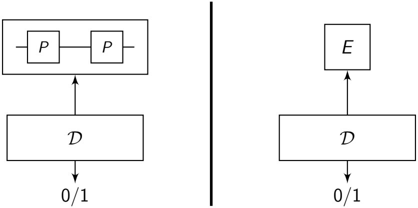
Random Square Permutation Problem

How many queries needs $\mathcal{D}$ to distinguish a random square permutation $P \circ P$ from a perfectly random permutation E?

Conjecture: indistinguishable up to $\sim 2^n$ queries

Best known attack: find a fixed point
($P \circ P$ has twice more fixed points than a random permutation)

Random *square* permutation vs. random permutation



Random Square Permutation Problem

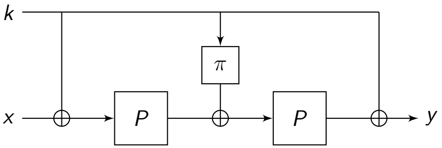
How many queries needs $\mathcal{D}$ to distinguish a random square permutation $P \circ P$ from a perfectly random permutation E?

Conjecture: indistinguishable up to $\sim 2^n$ queries

Best known attack: find a fixed point
($P \circ P$ has twice more fixed points than a random permutation)

Conclusion

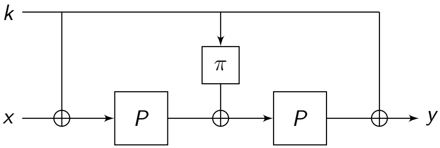
- minimal Even-Mansour cipher secure against generic attacks up to $\mathcal{O}(2^{\frac{2n}{3}})$ queries:



- first "beyond birthday-bound" security result for AES-like ciphers that does not require the "independent round keys" assumption
- open problems:
  - remove technical restrictions (mainly $\mathbb{F}_2$-linear key-schedule)
  - extend the result to $r \geq 3$ rounds! (generalization of the sum-capture problem?)

Conclusion

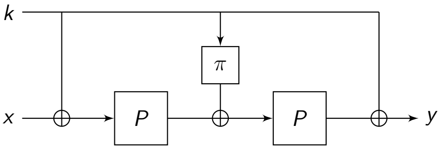
- minimal Even-Mansour cipher secure against generic attacks up to $\mathcal{O}(2^{\frac{2n}{3}})$ queries:



- first "beyond birthday-bound" security result for AES-like ciphers that does not require the "independent round keys" assumption
- open problems:
  - remove technical restrictions (mainly $\mathbb{F}_2$-linear key-schedule)
  - extend the result to $r \geq 3$ rounds!
    (generalization of the sum-capture problem?)

Conclusion

- minimal Even-Mansour cipher secure against generic attacks up to $\mathcal{O}(2^{\frac{2n}{3}})$ queries:



- first "beyond birthday-bound" security result for AES-like ciphers that does not require the "independent round keys" assumption
- open problems:
  - remove technical restrictions (mainly $\mathbb{F}_2$-linear key-schedule)
  - extend the result to $r \geq 3$ rounds!
    (generalization of the sum-capture problem?)

The end...

Thanks for your attention!

Comments or questions?

References I

László Babai.

The Fourier Transform and Equations over Finite Abelian Groups: An introduction to the method of trigonometric sums.

Lecture notes, December 1989.

Available at http://people.cs.uchicago.edu/~laci/reu02/fourier.pdf.

Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, François-Xavier Standaert, John P. Steinberger, and Elmar Tischhauser.

Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations - (Extended Abstract).

In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 45–62. Springer, 2012.

References II

Shan Chen and John Steinberger.
Tight Security Bounds for Key-Alternating Ciphers.
In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 327–350. Springer, 2014.
Full version available at `http://eprint.iacr.org/2013/222`.

Orr Dunkelman, Nathan Keller, and Adi Shamir.
Minimalism in Cryptography: The Even-Mansour Scheme Revisited.
In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 336–354. Springer, 2012.

Shimon Even and Yishay Mansour.
A Construction of a Cipher from a Single Pseudorandom Permutation.
Journal of Cryptology, 10(3):151–162, 1997.

References III

Rodolphe Lampe, Jacques Patarin, and Yannick Seurin.
An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher.
In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 278–295. Springer, 2012.

John Steinberger.
Improved Security Bounds for Key-Alternating Ciphers via Hellinger Distance.
IACR Cryptology ePrint Archive, Report 2012/481, 2012.
Available at `http://eprint.iacr.org/2012/481`.

John Steinberger.
Counting solutions to additive equations in random sets.
arXiv Report 1309.5582, 2013.
Available at `http://arxiv.org/abs/1309.5582`.