On the Provable Security of the Iterated Even-Mansour Cipher against Related-Key and Chosen-Key Attacks

Benoît Cogliati[1] and Yannick Seurin[2]

[1]Versailles University, France

[2]ANSSI, France

April 29, 2015 — EUROCRYPT 2015

Outline

Introduction: Key-Alternating Ciphers in the Random Permutation Model

Security Against Related-Key Attacks

Security Against Chosen-Key Attacks

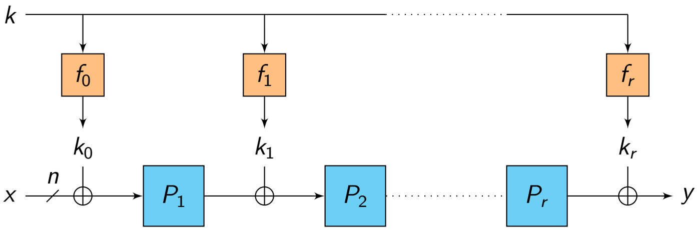
Outline

Introduction: Key-Alternating Ciphers in the Random Permutation Model

Security Against Related-Key Attacks

Security Against Chosen-Key Attacks

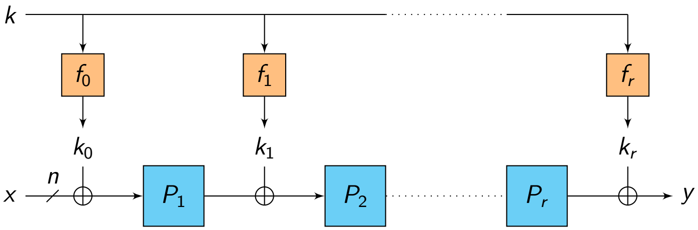
Key-Alternating Cipher (KAC): Definition



An r-round key-alternating cipher:

- plaintext $x \in \{0,1\}^n$, ciphertext $y \in \{0,1\}^n$
- master key $k \in \{0,1\}^\kappa$
- the P_i's are public permutations on $\{0,1\}^n$
- the f_i's are key derivation functions mapping k to n-bit "round keys"
- examples: most SPNs (AES, SERPENT, PRESENT, LED, . . .)

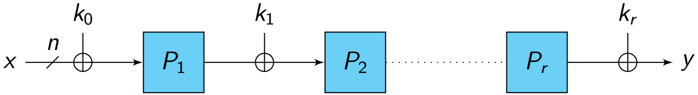
Key-Alternating Cipher (KAC): Definition



An r-round key-alternating cipher:

- plaintext $x \in \{0,1\}^n$, ciphertext $y \in \{0,1\}^n$
- master key $k \in \{0,1\}^\kappa$
- the P_i's are public permutations on $\{0,1\}^n$
- the f_i's are key derivation functions mapping k to n-bit "round keys"
- examples: most SPNs (AES, SERPENT, PRESENT, LED, . . .)

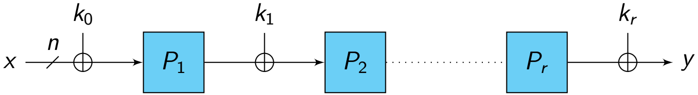
Various Key-Schedule Types



Round keys can be:

- independent (total key-length $\kappa = (r+1)n$)
- derived from an n-bit master key ($\kappa = n$), e.g.
  - trivial key-schedule: $(k, k, \ldots, k)$
  - more complex: $(f_0(k), f_1(k), \ldots, f_r(k))$
- anything else (e.g. $2n$-bit master key (k_0, k_1) and round keys $(k_0, k_1, k_0, k_1, \ldots)$ as in LED-128)

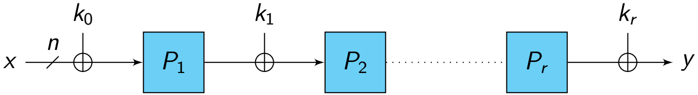
Various Key-Schedule Types



Round keys can be:

- independent (total key-length $\kappa = (r+1)n$)
- derived from an n-bit master key ($\kappa = n$), e.g.
  - trivial key-schedule: $(k, k, \ldots, k)$
  - more complex: $(f_0(k), f_1(k), \ldots, f_r(k))$
- anything else (e.g. $2n$-bit master key (k_0, k_1) and round keys $(k_0, k_1, k_0, k_1, \ldots)$ as in LED-128)

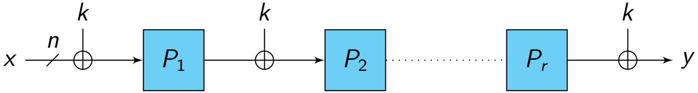
Various Key-Schedule Types



Round keys can be:

- independent (total key-length $\kappa = (r+1)n$)
- derived from an n-bit master key ($\kappa = n$), e.g.
    - trivial key-schedule: $(k, k, \ldots, k)$
    - more complex: $(f_0(k), f_1(k), \ldots, f_r(k))$
- anything else (e.g. $2n$-bit master key (k_0, k_1) and round keys $(k_0, k_1, k_0, k_1, \ldots)$ as in LED-128)

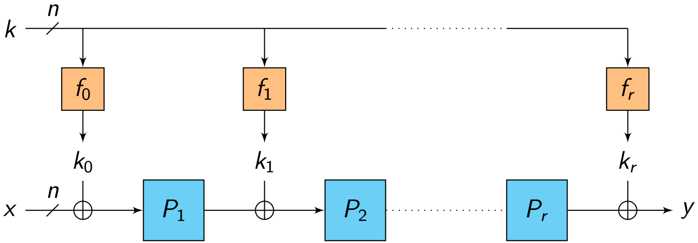
Various Key-Schedule Types



Round keys can be:

- independent (total key-length $\kappa = (r+1)n$)
- derived from an n-bit master key ($\kappa = n$), e.g.
  - trivial key-schedule: $(k, k, \ldots, k)$
  - more complex: $(f_0(k), f_1(k), \ldots, f_r(k))$
- anything else (e.g. $2n$-bit master key (k_0, k_1) and round keys $(k_0, k_1, k_0, k_1, \ldots)$ as in LED-128)

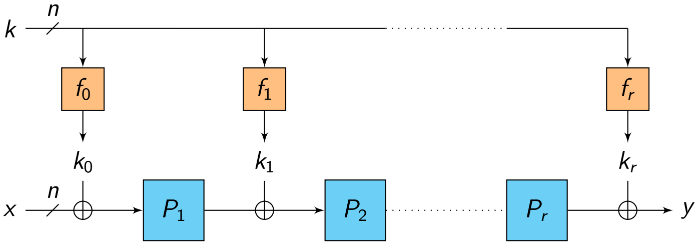
Various Key-Schedule Types



Round keys can be:

- independent (total key-length $\kappa = (r+1)n$)
- derived from an n-bit master key ($\kappa = n$), e.g.
    - trivial key-schedule: $(k, k, \ldots, k)$
    - more complex: $(f_0(k), f_1(k), \ldots, f_r(k))$
- anything else (e.g. $2n$-bit master key (k_0, k_1) and round keys $(k_0, k_1, k_0, k_1, \ldots)$ as in LED-128)

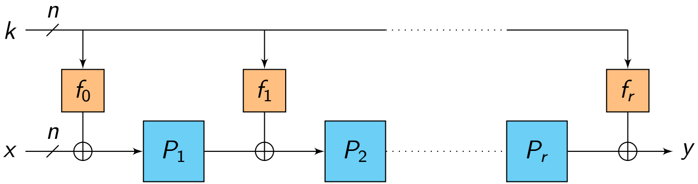
Various Key-Schedule Types



Round keys can be:

- independent (total key-length $\kappa = (r+1)n$)
- derived from an n-bit master key ($\kappa = n$), e.g.
    - trivial key-schedule: $(k, k, \ldots, k)$
    - more complex: $(f_0(k), f_1(k), \ldots, f_r(k))$
- anything else (e.g. $2n$-bit master key (k_0, k_1) and round keys $(k_0, k_1, k_0, k_1, \ldots)$ as in LED-128)

Proving the Security of KACs

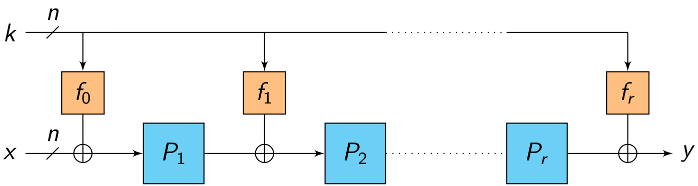


Question

How can we “prove” security?

- 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 KACs

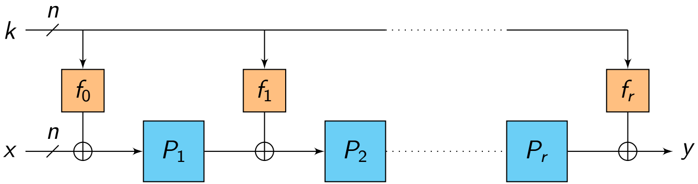


Question

How can we "prove" security?

- 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 KACs

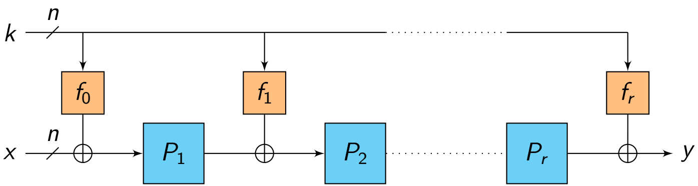


Question

How can we “prove” security?

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

Proving the Security of KACs

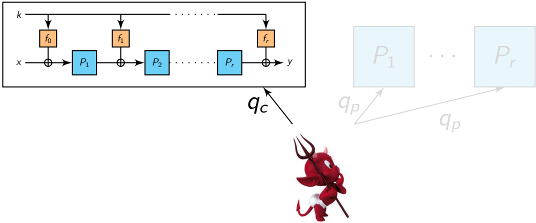


Question

How can we “prove” security?

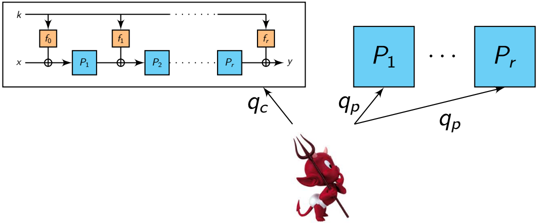
- against a general adversary:
  ⇒ too hard (unconditional complexity lower bound!)
- against specific attacks (differential, linear. . .):
  ⇒ use specific design of $P_1, \dots, P_r$ (count active S-boxes, etc.)
- against generic attacks:
  ⇒ Random Permutation Model for $P_1, \dots, P_r$

Analyzing KACs in the Random Permutation Model



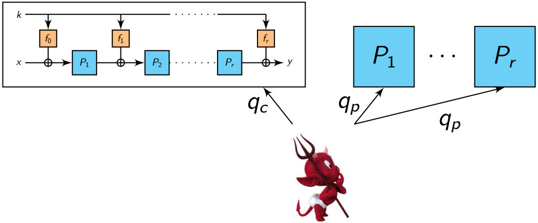
- the P_i's are modeled as public random permutation oracles to which the adversary can only make black-box queries (both to P_i and P_i^{-1})
- adversary cannot exploit any weakness of the P_i's ⇒ generic attacks
- trades complexity for randomness ($\simeq$ Random Oracle Model)
- complexity measure of the adversary:
  - $q_c = \#$ queries to the cipher = plaintext/ciphertext pairs (data D)
  - $q_p = \#$ queries to each internal permutation oracle (time T)
  - but otherwise computationally unbounded
- ⇒ information-theoretic proof of security

Analyzing KACs in the Random Permutation Model



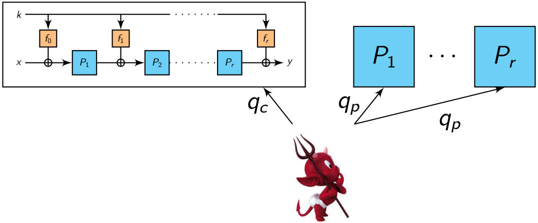
- the P_i's are modeled as public random permutation oracles to which the adversary can only make black-box queries (both to P_i and P_i^{-1})
- adversary cannot exploit any weakness of the P_i's ⇒ generic attacks
- trades complexity for randomness ($\simeq$ Random Oracle Model)
- complexity measure of the adversary:
  - q_c = # queries to the cipher = plaintext/ciphertext pairs (data D)
  - q_p = # queries to each internal permutation oracle (time T)
  - but otherwise computationally unbounded
- ⇒ information-theoretic proof of security

Analyzing KACs in the Random Permutation Model



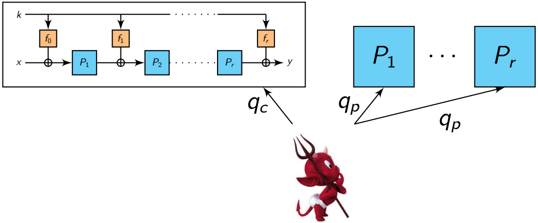
- the P_i's are modeled as public random permutation oracles to which the adversary can only make black-box queries (both to P_i and P_i^{-1})
- adversary cannot exploit any weakness of the P_i's ⇒ generic attacks
- trades complexity for randomness ($\simeq$ Random Oracle Model)
- complexity measure of the adversary:
  - $q_c = \#$ queries to the cipher = plaintext/ciphertext pairs (data D)
  - $q_p = \#$ queries to each internal permutation oracle (time T)
  - but otherwise computationally unbounded
- ⇒ information-theoretic proof of security

Analyzing KACs in the Random Permutation Model



- the P_i's are modeled as public random permutation oracles to which the adversary can only make black-box queries (both to P_i and P_i^{-1})
- adversary cannot exploit any weakness of the P_i's ⇒ generic attacks
- trades complexity for randomness ($\simeq$ Random Oracle Model)
- complexity measure of the adversary:
  - $q_c = \#$ queries to the cipher = plaintext/ciphertext pairs (data D)
  - $q_p = \#$ queries to each internal permutation oracle (time T)
  - but otherwise computationally unbounded
- ⇒ information-theoretic proof of security

Analyzing KACs in the Random Permutation Model

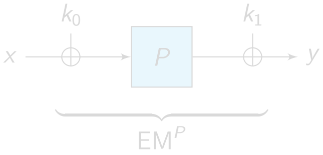


- the P_i's are modeled as public random permutation oracles to which the adversary can only make black-box queries (both to P_i and P_i^{-1})
- adversary cannot exploit any weakness of the P_i's $\Rightarrow$ generic attacks
- trades complexity for randomness ($\simeq$ Random Oracle Model)
- complexity measure of the adversary:
  - q_c = # queries to the cipher = plaintext/ciphertext pairs (data D)
  - q_p = # queries to each internal permutation oracle (time T)
  - but otherwise computationally unbounded
- $\Rightarrow$ information-theoretic proof of security

Analyzing KACs in the Random Permutation Model

Even and Mansour seminal work:

- this model was first proposed by Even and Mansour at ASIACRYPT '91 for $r = 1$ round
- they showed that the simple cipher $k_1 \oplus P(k_0 \oplus x)$ is a secure PRP up to $\sim 2^{\frac{n}{2}}$ queries of the adversary to P and to the cipher
- similar result when $k_0 = k_1$ [KR01, DKS12]

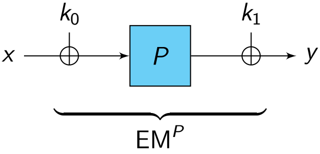


- improved bound as r increases: PRP up to $\sim 2^{\frac{rn}{r+1}}$ queries [CS14]

Analyzing KACs in the Random Permutation Model

Even and Mansour seminal work:

- this model was first proposed by Even and Mansour at ASIACRYPT '91 for $r = 1$ round
- they showed that the simple cipher $k_1 \oplus P(k_0 \oplus x)$ is a secure PRP up to $\sim 2^{\frac{n}{2}}$ queries of the adversary to P and to the cipher
- similar result when $k_0 = k_1$ [KR01, DKS12]

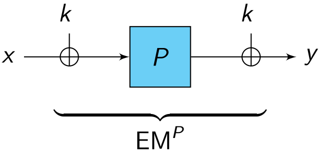


- improved bound as r increases: PRP up to $\sim 2^{\frac{rn}{r+1}}$ queries [CS14]

Analyzing KACs in the Random Permutation Model

Even and Mansour seminal work:

- this model was first proposed by Even and Mansour at ASIACRYPT '91 for $r = 1$ round
- they showed that the simple cipher $k_1 \oplus P(k_0 \oplus x)$ is a secure PRP up to $\sim 2^{\frac{n}{2}}$ queries of the adversary to P and to the cipher
- similar result when $k_0 = k_1$ [KR01, DKS12]

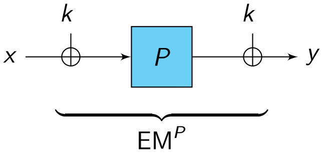


- improved bound as r increases: PRP up to $\sim 2^{\frac{rn}{r+1}}$ queries [CS14]

Analyzing KACs in the Random Permutation Model

Even and Mansour seminal work:

- this model was first proposed by Even and Mansour at ASIACRYPT '91 for $r = 1$ round
- they showed that the simple cipher $k_1 \oplus P(k_0 \oplus x)$ is a secure PRP up to $\sim 2^{\frac{n}{2}}$ queries of the adversary to P and to the cipher
- similar result when $k_0 = k_1$ [KR01, DKS12]



- improved bound as r increases: PRP up to $\sim 2^{\frac{rn}{r+1}}$ queries [CS14]

Outline

Introduction: Key-Alternating Ciphers in the Random Permutation Model

Security Against Related-Key Attacks

Security Against Chosen-Key Attacks

Related-Key Attacks

The Related-Key Attack Model [BK03]:

- stronger adversarial model: the adversary can specify Related-Key Deriving (RKD) functions ϕ and receive $E_{\phi(k)}(x)$ and/or $E^{-1}_{\phi(k)}(y)$
- the block cipher should behave as an ideal cipher (an independent random permutation for each key)
- impossibility results for too "large" sets of RKDs
- positive results for limited sets of RKDs or using number-theoretic constructions
- we will consider XOR-RKAs: the set of RKD functions is

$$\{\phi_\Delta : k \mapsto k \oplus \Delta, \Delta \in \{0,1\}^\kappa\}$$

Related-Key Attacks

The Related-Key Attack Model [BK03]:

- stronger adversarial model: the adversary can specify Related-Key Deriving (RKD) functions ϕ and receive $E_{\phi(k)}(x)$ and/or $E^{-1}_{\phi(k)}(y)$
- the block cipher should behave as an ideal cipher (an independent random permutation for each key)
- impossibility results for too "large" sets of RKDs
- positive results for limited sets of RKDs or using number-theoretic constructions
- we will consider XOR-RKAs: the set of RKD functions is

$$\{\phi_\Delta : k \mapsto k \oplus \Delta, \Delta \in \{0,1\}^\kappa\}$$

Related-Key Attacks

The Related-Key Attack Model [BK03]:

- stronger adversarial model: the adversary can specify Related-Key Deriving (RKD) functions ϕ and receive $E_{\phi(k)}(x)$ and/or $E^{-1}_{\phi(k)}(y)$
- the block cipher should behave as an ideal cipher (an independent random permutation for each key)
- impossibility results for too "large" sets of RKDs
- positive results for limited sets of RKDs or using number-theoretic constructions
- we will consider XOR-RKAs: the set of RKD functions is

$$\{\phi_\Delta : k \mapsto k \oplus \Delta, \Delta \in \{0,1\}^\kappa\}$$

Related-Key Attacks

The Related-Key Attack Model [BK03]:

- stronger adversarial model: the adversary can specify Related-Key Deriving (RKD) functions ϕ and receive $E_{\phi(k)}(x)$ and/or $E^{-1}_{\phi(k)}(y)$
- the block cipher should behave as an ideal cipher (an independent random permutation for each key)
- impossibility results for too "large" sets of RKDs
- positive results for limited sets of RKDs or using number-theoretic constructions
- we will consider XOR-RKAs: the set of RKD functions is

$$\{\phi_\Delta : k \mapsto k \oplus \Delta, \Delta \in \{0,1\}^\kappa\}$$

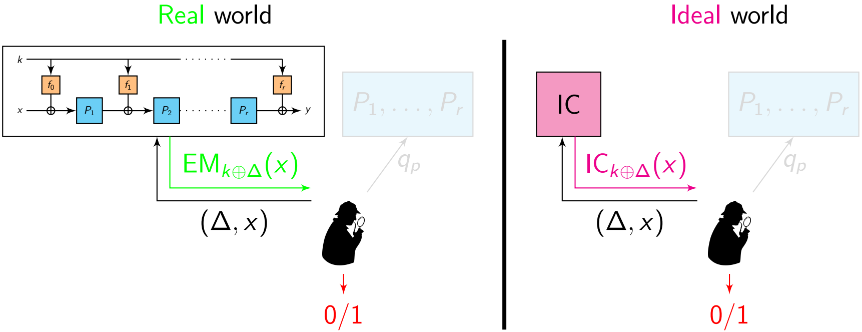
Related-Key Attacks

The Related-Key Attack Model [BK03]:

- stronger adversarial model: the adversary can specify Related-Key Deriving (RKD) functions ϕ and receive $E_{\phi(k)}(x)$ and/or $E^{-1}_{\phi(k)}(y)$
- the block cipher should behave as an ideal cipher (an independent random permutation for each key)
- impossibility results for too "large" sets of RKDs
- positive results for limited sets of RKDs or using number-theoretic constructions
- we will consider XOR-RKAs: the set of RKD functions is

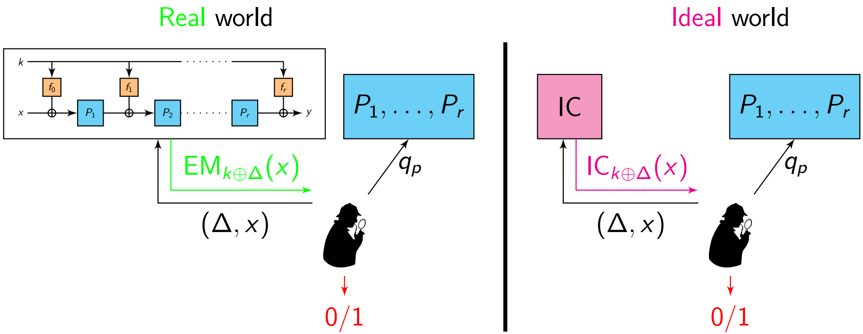
$$\{\phi_\Delta : k \mapsto k \oplus \Delta, \Delta \in \{0,1\}^\kappa\}$$

XOR-RKAs against the IEM Cipher: Formalization



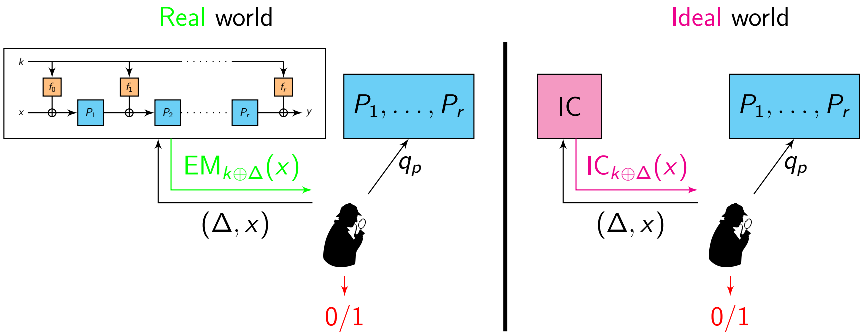
- real world: IEM cipher with a random key $k \leftarrow_{\$} \{0,1\}^{\kappa}$
- ideal world: ideal cipher IC independent from $P_1, \ldots, P_r$
- Rand. Perm. Model: $\mathcal{D}$ has oracle access to $P_1, \ldots, P_r$ in both worlds
- q_c queries to the IEM/IC and q_p queries to each inner perm.

XOR-RKAs against the IEM Cipher: Formalization



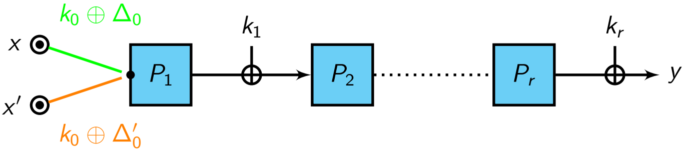
- real world: IEM cipher with a random key $k \leftarrow_{\$} \{0,1\}^{\kappa}$
- ideal world: ideal cipher IC independent from $P_1, \dots, P_r$
- Rand. Perm. Model: $\mathcal{D}$ has oracle access to $P_1, \dots, P_r$ in both worlds
- q_c queries to the IEM/IC and q_p queries to each inner perm.

XOR-RKAs against the IEM Cipher: Formalization



- real world: IEM cipher with a random key $k \leftarrow_\$ \{0,1\}^\kappa$
- ideal world: ideal cipher IC independent from $P_1, \ldots, P_r$
- Rand. Perm. Model: $\mathcal{D}$ has oracle access to $P_1, \ldots, P_r$ in both worlds
- q_c queries to the IEM/IC and q_p queries to each inner perm.

First Observation: Independent Round Keys Fails



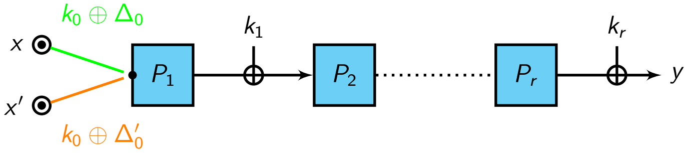
RK Distinguisher for independent round keys:

- query $((\Delta_0, 0, \ldots, 0), x)$ and $((\Delta'_0, 0, \ldots, 0), x')$ such that

$$x \oplus \Delta_0 = x' \oplus \Delta'_0$$

- check that the outputs are equal
- holds with proba. 1 for the IEM cipher
- holds with proba. 2^{-n} for an ideal cipher
- $\Rightarrow$ we will consider "dependent" round keys (in part. $(k, k, \ldots, k)$)

First Observation: Independent Round Keys Fails



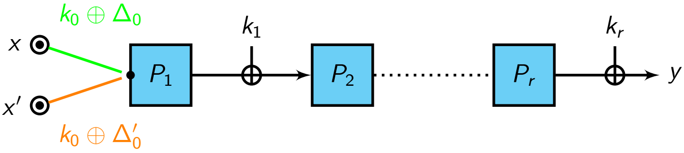
RK Distinguisher for independent round keys:

- query $((\Delta_0, 0, \ldots, 0), x)$ and $((\Delta_0', 0, \ldots, 0), x')$ such that

$$x \oplus \Delta_0 = x' \oplus \Delta_0'$$

- check that the outputs are equal
- holds with proba. 1 for the IEM cipher
- holds with proba. 2^{-n} for an ideal cipher
- $\Rightarrow$ we will consider "dependent" round keys (in part. $(k, k, \ldots, k)$)

First Observation: Independent Round Keys Fails



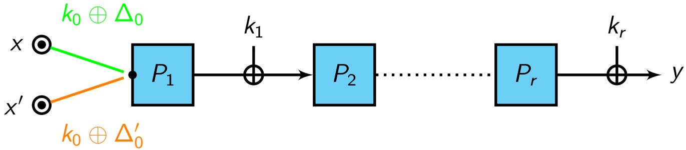
RK Distinguisher for independent round keys:

- query $((\Delta_0, 0, \ldots, 0), x)$ and $((\Delta'_0, 0, \ldots, 0), x')$ such that

$$x \oplus \Delta_0 = x' \oplus \Delta'_0$$

- check that the outputs are equal
- holds with proba. 1 for the IEM cipher
- holds with proba. 2^{-n} for an ideal cipher
- $\Rightarrow$ we will consider "dependent" round keys (in part. $(k, k, \ldots, k)$)

First Observation: Independent Round Keys Fails



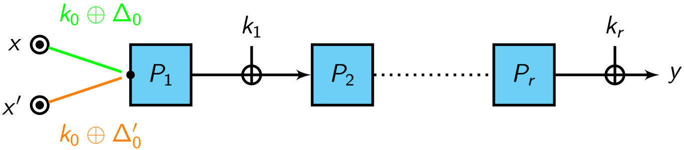
RK Distinguisher for independent round keys:

- query $((\Delta_0, 0, \ldots, 0), x)$ and $((\Delta'_0, 0, \ldots, 0), x')$ such that

$$x \oplus \Delta_0 = x' \oplus \Delta'_0$$

- check that the outputs are equal
- holds with proba. 1 for the IEM cipher
- holds with proba. 2^{-n} for an ideal cipher
- $\Rightarrow$ we will consider "dependent" round keys (in part. $(k, k, \ldots, k)$)

First Observation: Independent Round Keys Fails



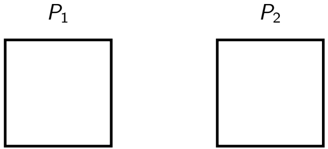
RK Distinguisher for independent round keys:

- query $((\Delta_0, 0, \dots, 0), x)$ and $((\Delta'_0, 0, \dots, 0), x')$ such that

$$x \oplus \Delta_0 = x' \oplus \Delta'_0$$

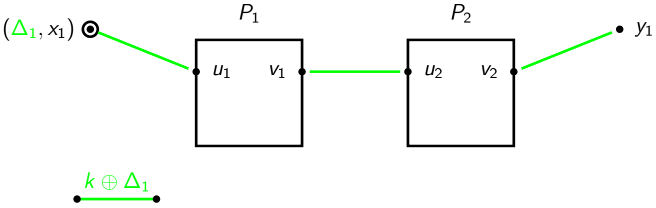
- check that the outputs are equal
- holds with proba. 1 for the IEM cipher
- holds with proba. 2^{-n} for an ideal cipher
- $\Rightarrow$ we will consider "dependent" round keys (in part. $(k, k, \dots, k)$)

An Attack for Two Rounds, Trivial Key-Schedule



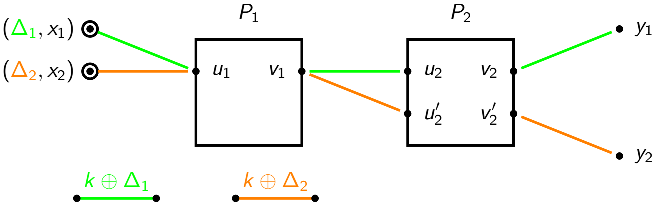
- 4 queries to the RK oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the 2-round IEM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule
- has been extended to a key-recovery attack (using a modular addition RKA instead of a XOR-RKA)[Kar15]

An Attack for Two Rounds, Trivial Key-Schedule



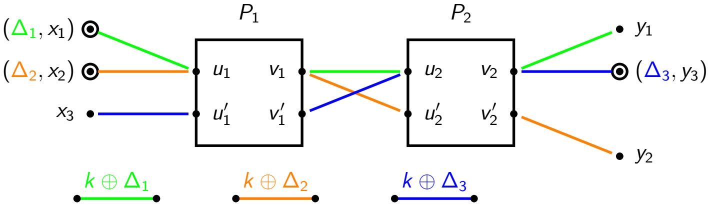
- 4 queries to the RK oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the 2-round IEM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule
- has been extended to a key-recovery attack (using a modular addition RKA instead of a XOR-RKA)[Kar15]

An Attack for Two Rounds, Trivial Key-Schedule



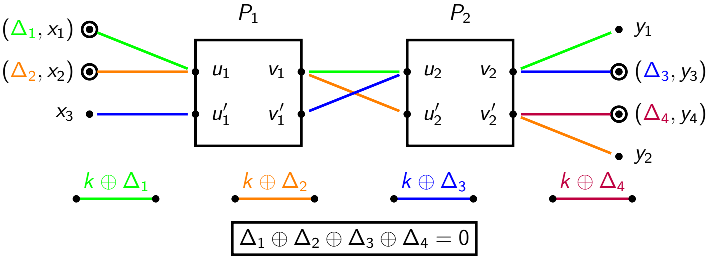
- 4 queries to the RK oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the 2-round IEM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule
- has been extended to a key-recovery attack (using a modular addition RKA instead of a XOR-RKA)[Kar15]

An Attack for Two Rounds, Trivial Key-Schedule



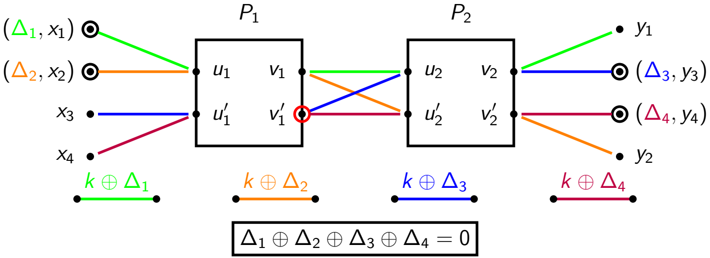
- 4 queries to the RK oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the 2-round IEM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule
- has been extended to a key-recovery attack (using a modular addition RKA instead of a XOR-RKA)[Kar15]

An Attack for Two Rounds, Trivial Key-Schedule



- 4 queries to the RK oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the 2-round IEM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule
- has been extended to a key-recovery attack (using a modular addition RKA instead of a XOR-RKA)[Kar15]

An Attack for Two Rounds, Trivial Key-Schedule

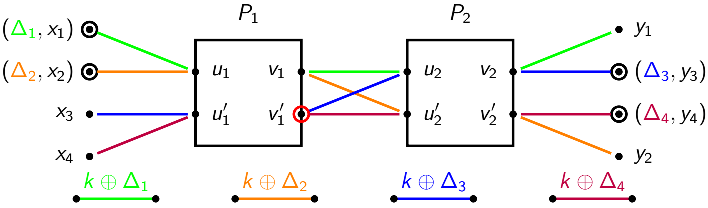


$$\boxed{\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0}$$

Check that $x_3 \oplus x_4 = \Delta_3 \oplus \Delta_4$ $(*)$

- 4 queries to the RK oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the 2-round IEM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule
- has been extended to a key-recovery attack (using a modular addition RKA instead of a XOR-RKA)[Kar15]

An Attack for Two Rounds, Trivial Key-Schedule

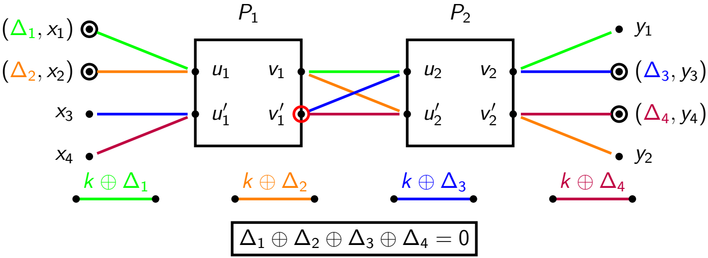


$$\boxed{\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0}$$

Check that $x_3 \oplus x_4 = \Delta_3 \oplus \Delta_4$ $(*)$

- 4 queries to the RK oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the 2-round IEM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule
- has been extended to a key-recovery attack (using a modular addition RKA instead of a XOR-RKA)[Kar15]

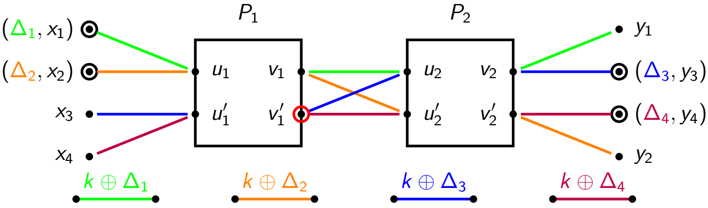
An Attack for Two Rounds, Trivial Key-Schedule



Check that $x_3 \oplus x_4 = \Delta_3 \oplus \Delta_4$ $(*)$

- 4 queries to the RK oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the 2-round IEM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule
- has been extended to a key-recovery attack (using a modular addition RKA instead of a XOR-RKA)[Kar15]

An Attack for Two Rounds, Trivial Key-Schedule

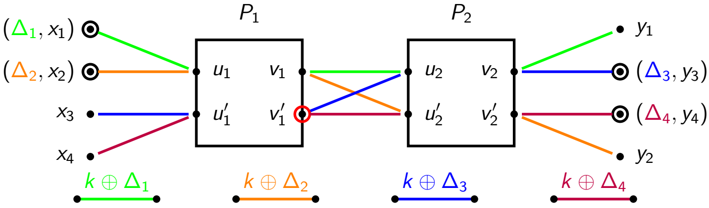


$$\boxed{\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0}$$

Check that $x_3 \oplus x_4 = \Delta_3 \oplus \Delta_4$ $(*)$

- 4 queries to the RK oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the 2-round IEM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule
- has been extended to a key-recovery attack (using a modular addition RKA instead of a XOR-RKA)[Kar15]

An Attack for Two Rounds, Trivial Key-Schedule

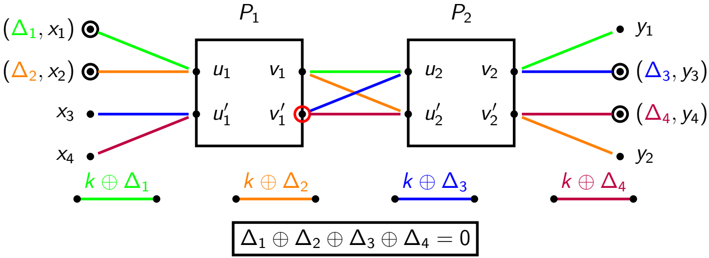


$$\boxed{\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0}$$

Check that $x_3 \oplus x_4 = \Delta_3 \oplus \Delta_4$ $(*)$

- 4 queries to the RK oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the 2-round IEM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule
- has been extended to a key-recovery attack (using a modular addition RKA instead of a XOR-RKA)[Kar15]

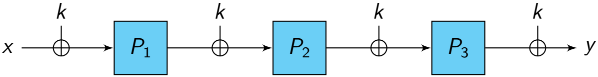
An Attack for Two Rounds, Trivial Key-Schedule



Check that $x_3 \oplus x_4 = \Delta_3 \oplus \Delta_4$ (∗)

- 4 queries to the RK oracle, 0 queries to P_1, P_2
- (∗) holds with proba. 1 for the 2-round IEM cipher
- (∗) holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule
- has been extended to a key-recovery attack (using a modular addition RKA instead of a XOR-RKA)[Kar15]

Security for Three Rounds, Trivial Key-Schedule



Theorem (Cogliati-Seurin [CS15])

For the 3-round IEM cipher with the trivial key-schedule:

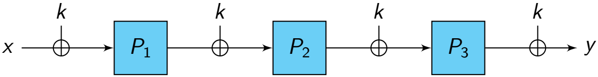
$$\mathbf{Adv}^{\text{xor-rka}}_{\mathsf{EM}[n,3]}(q_c, q_p) \leq \frac{6 q_c q_p}{2^n} + \frac{4 q_c^2}{2^n}.$$

Proof sketch:

- $\mathcal{D}$ can create forward collisions at P_1 or backward collisions at P_3
- but proba. to create a collision at P_2 is $\lesssim q_c^2/2^n$
- no collision at P_2

  $\Rightarrow \sim$ single-key security of 1-round EM $\lesssim q_c q_p/2^n$

Security for Three Rounds, Trivial Key-Schedule



Theorem (Cogliati-Seurin [CS15])

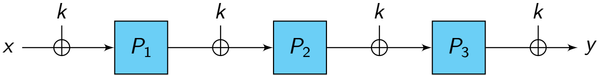
For the 3-round IEM cipher with the trivial key-schedule:

$$\mathbf{Adv}^{\text{xor-rka}}_{\mathsf{EM}[n,3]}(q_c, q_p) \le \frac{6q_cq_p}{2^n} + \frac{4q_c^2}{2^n}.$$

Proof sketch:

- $\mathcal{D}$ can create forward collisions at P_1 or backward collisions at P_3
- but proba. to create a collision at P_2 is $\lesssim q_c^2/2^n$
- no collision at P_2
  $\Rightarrow \sim$ single-key security of 1-round EM $\lesssim q_cq_p/2^n$

Security for Three Rounds, Trivial Key-Schedule



Theorem (Cogliati-Seurin [CS15])

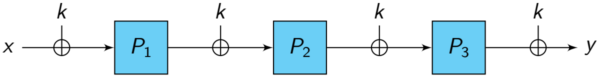
For the 3-round IEM cipher with the trivial key-schedule:

$$\mathbf{Adv}^{\text{xor-rka}}_{\mathsf{EM}[n,3]}(q_c, q_p) \leq \frac{6q_c q_p}{2^n} + \frac{4q_c^2}{2^n}.$$

Proof sketch:

- $\mathcal{D}$ can create forward collisions at P_1 or backward collisions at P_3
- but proba. to create a collision at P_2 is $\lesssim q_c^2/2^n$
- no collision at P_2
  $\Rightarrow \sim$ single-key security of 1-round EM $\lesssim q_c q_p/2^n$

Security for Three Rounds, Trivial Key-Schedule



Theorem (Cogliati-Seurin [CS15])

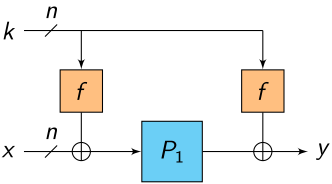
For the 3-round IEM cipher with the trivial key-schedule:

$$\mathbf{Adv}^{\text{xor-rka}}_{\mathsf{EM}[n,3]}(q_c, q_p) \leq \frac{6q_c q_p}{2^n} + \frac{4q_c^2}{2^n}.$$

Proof sketch:

- $\mathcal{D}$ can create forward collisions at P_1 or backward collisions at P_3
- but proba. to create a collision at P_2 is $\lesssim q_c^2/2^n$
- no collision at P_2
  $\Rightarrow \sim$ single-key security of 1-round EM $\lesssim q_c q_p/2^n$

Security for One Round and a Nonlinear Key-Schedule



Theorem (Cogliati-Seurin [CS15])

For the 1-round EM cipher with key-schedule $f = (f_0, f_1)$:

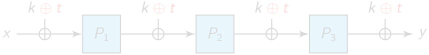
$$\mathbf{Adv}^{\text{xor-rka}}_{\text{EM}[n,1,f]}(q_c, q_p) \le \frac{2q_c q_p}{2^n} + \frac{\delta(f) q_c^2}{2^n},$$

where $\delta(f) = \max_{a,b\in\{0,1\}^n, a\neq 0} |\{x \in \{0,1\}^n : f(x \oplus a) \oplus f(x) = b\}|$.
($\delta(f) = 2$ for an APN permutation.)

Some Observations

Application to tweakable block ciphers:

- from any XOR-RKA secure block cipher E, one can construct a tweakable block cipher [LRW02, BK03]



- Similar in spirit to the TWEAKEY framework from Jean et al [JNP14].

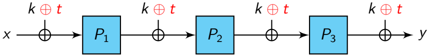
Independent work by Farshim and Procter at FSE 2015 [FP15]:

- similar result for 3 rounds (slightly worse bound, game-based proof)
- 2 rounds: XOR-RKA security against chosen-plaintext attacks
- 1 round: RKA-security for more limited sets of RKDs

Some Observations

Application to tweakable block ciphers:

- from any XOR-RKA secure block cipher E, one can construct a tweakable block cipher [LRW02, BK03]



- Similar in spirit to the TWEAKEY framework from Jean et al [JNP14].

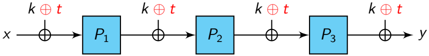
Independent work by Farshim and Procter at FSE 2015 [FP15]:

- similar result for 3 rounds (slightly worse bound, game-based proof)
- 2 rounds: XOR-RKA security against chosen-plaintext attacks
- 1 round: RKA-security for more limited sets of RKDs

Some Observations

Application to tweakable block ciphers:

- from any XOR-RKA secure block cipher E, one can construct a tweakable block cipher [LRW02, BK03]



- Similar in spirit to the TWEAKEY framework from Jean et al [JNP14].

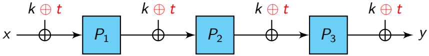
Independent work by Farshim and Procter at FSE 2015 [FP15]:

- similar result for 3 rounds (slightly worse bound, game-based proof)
- 2 rounds: XOR-RKA security against chosen-plaintext attacks
- 1 round: RKA-security for more limited sets of RKDs

Some Observations

Application to tweakable block ciphers:

- from any XOR-RKA secure block cipher E, one can construct a tweakable block cipher [LRW02, BK03]



- Similar in spirit to the TWEAKEY framework from Jean et al [JNP14].

Independent work by Farshim and Procter at FSE 2015 [FP15]:

- similar result for 3 rounds (slightly worse bound, game-based proof)
- 2 rounds: XOR-RKA security against chosen-plaintext attacks
- 1 round: RKA-security for more limited sets of RKDs

Outline

Introduction: Key-Alternating Ciphers in the Random Permutation Model

Security Against Related-Key Attacks

Security Against Chosen-Key Attacks

Formalizing Chosen-Key Attacks

- informal goal: find tuples of key/pt/ct (k_i, x_i, y_i) with a property which is hard to satisfy for an ideal cipher
- no formal definition for a single, completely instantiated block cipher E
- simply because, e.g., $E_0(0)$ has a specific, non-random value...
- OK this does not count
- but what counts as a chosen-key attack exactly?
- rigorous definition possible for a family of block ciphers based on some underlying ideal primitive
- e.g., IEM cipher based on a tuple of random permutations!
- our definitions are adapted from [CGH98]

Formalizing Chosen-Key Attacks

- informal goal: find tuples of key/pt/ct (k_i, x_i, y_i) with a property which is hard to satisfy for an ideal cipher
- no formal definition for a single, completely instantiated block cipher E
- simply because, e.g., $E_0(0)$ has a specific, non-random value...
- OK this does not count
- but what counts as a chosen-key attack exactly?
- rigorous definition possible for a family of block ciphers based on some underlying ideal primitive
- e.g., IEM cipher based on a tuple of random permutations!
- our definitions are adapted from [CGH98]

Formalizing Chosen-Key Attacks

- informal goal: find tuples of key/pt/ct (k_i, x_i, y_i) with a property which is hard to satisfy for an ideal cipher
- no formal definition for a single, completely instantiated block cipher E
- simply because, e.g., $E_0(0)$ has a specific, non-random value...
- OK this does not count
- but what counts as a chosen-key attack exactly?
- rigorous definition possible for a family of block ciphers based on some underlying ideal primitive
- e.g., IEM cipher based on a tuple of random permutations!
- our definitions are adapted from [CGH98]

Formalizing Chosen-Key Attacks

- informal goal: find tuples of key/pt/ct (k_i, x_i, y_i) with a property which is hard to satisfy for an ideal cipher
- no formal definition for a single, completely instantiated block cipher E
- simply because, e.g., $E_0(0)$ has a specific, non-random value. . .
- OK this does not count
- but what counts as a chosen-key attack exactly?
- rigorous definition possible for a family of block ciphers based on some underlying ideal primitive
- e.g., IEM cipher based on a tuple of random permutations!
- our definitions are adapted from [CGH98]

Formalizing Chosen-Key Attacks

- informal goal: find tuples of key/pt/ct (k_i, x_i, y_i) with a property which is hard to satisfy for an ideal cipher
- no formal definition for a single, completely instantiated block cipher E
- simply because, e.g., $E_0(0)$ has a specific, non-random value. . .
- OK this does not count
- but what counts as a chosen-key attack exactly?
- rigorous definition possible for a family of block ciphers based on some underlying ideal primitive
- e.g., IEM cipher based on a tuple of random permutations!
- our definitions are adapted from [CGH98]

Formalizing Chosen-Key Attacks

- informal goal: find tuples of key/pt/ct (k_i, x_i, y_i) with a property which is hard to satisfy for an ideal cipher
- no formal definition for a single, completely instantiated block cipher E
- simply because, e.g., $E_0(0)$ has a specific, non-random value...
- OK this does not count
- but what counts as a chosen-key attack exactly?
- rigorous definition possible for a family of block ciphers based on some underlying ideal primitive
- e.g., IEM cipher based on a tuple of random permutations!
- our definitions are adapted from [CGH98]

Formalizing Chosen-Key Attacks

- informal goal: find tuples of key/pt/ct (k_i, x_i, y_i) with a property which is hard to satisfy for an ideal cipher
- no formal definition for a single, completely instantiated block cipher E
- simply because, e.g., $E_0(0)$ has a specific, non-random value. . .
- OK this does not count
- but what counts as a chosen-key attack exactly?
- rigorous definition possible for a family of block ciphers based on some underlying ideal primitive
- e.g., IEM cipher based on a tuple of random permutations!
- our definitions are adapted from [CGH98]

Formalizing Chosen-Key Attacks

- informal goal: find tuples of key/pt/ct (k_i, x_i, y_i) with a property which is hard to satisfy for an ideal cipher
- no formal definition for a single, completely instantiated block cipher E
- simply because, e.g., $E_0(0)$ has a specific, non-random value...
- OK this does not count
- but what counts as a chosen-key attack exactly?
- rigorous definition possible for a family of block ciphers based on some underlying ideal primitive
- e.g., IEM cipher based on a tuple of random permutations!
- our definitions are adapted from [CGH98]

Formalizing Chosen-Key Attacks

Definition (Evasive relation)

An m-ary relation $\mathcal{R}$ is (q, ε)-evasive (w.r.t. an ideal cipher E) if any adversary $\mathcal{A}$ making at most q queries to E finds triples $(k_1, x_1, y_1), \ldots, (k_m, x_m, y_m)$ (with $E_{k_i}(x_i) = y_i$) satisfying $\mathcal{R}$ with probability at most ε.

Example

- consider E in Davies-Meyer mode $f(k, x) := E_k(x) \oplus x$
- finding a preimage of 0 for f is a unary $(q, \mathcal{O}(\frac{q}{2^n}))$-evasive relation for E [BRS02]
- finding a collision for f is a binary $\left(q, \mathcal{O}(\frac{q^2}{2^n})\right)$-evasive relation for E [BRS02]
- for BC-based hashing, most hash function security notions can be recast as evasive relations for the underlying BC

Formalizing Chosen-Key Attacks

Definition (Evasive relation)

An m-ary relation $\mathcal{R}$ is (q, ε)-evasive (w.r.t. an ideal cipher E) if any adversary $\mathcal{A}$ making at most q queries to E finds triples $(k_1, x_1, y_1), \ldots,$ (k_m, x_m, y_m) (with $E_{k_i}(x_i) = y_i$) satisfying $\mathcal{R}$ with probability at most ε.

Example

- consider E in Davies-Meyer mode $f(k,x) := E_k(x) \oplus x$
- finding a preimage of 0 for f is a unary $(q, \mathcal{O}(\frac{q}{2^n}))$-evasive relation for E [BRS02]
- finding a collision for f is a binary $\left(q, \mathcal{O}(\frac{q^2}{2^n})\right)$-evasive relation for E [BRS02]
- for BC-based hashing, most hash function security notions can be recast as evasive relations for the underlying BC

Formalizing Chosen-Key Attacks

Definition (Evasive relation)

An m-ary relation $\mathcal{R}$ is (q, ε)-evasive (w.r.t. an ideal cipher E) if any adversary $\mathcal{A}$ making at most q queries to E finds triples $(k_1, x_1, y_1), \ldots, (k_m, x_m, y_m)$ (with $E_{k_i}(x_i) = y_i$) satisfying $\mathcal{R}$ with probability at most ε.

Example

- consider E in Davies-Meyer mode $f(k, x) := E_k(x) \oplus x$
- finding a preimage of 0 for f is a unary $(q, \mathcal{O}(\frac{q}{2^n}))$-evasive relation for E [BRS02]
- finding a collision for f is a binary $\left(q, \mathcal{O}(\frac{q^2}{2^n})\right)$-evasive relation for E [BRS02]
- for BC-based hashing, most hash function security notions can be recast as evasive relations for the underlying BC

Formalizing Chosen-Key Attacks

Definition (Evasive relation)

An m-ary relation $\mathcal{R}$ is (q, ε)-evasive (w.r.t. an ideal cipher E) if any adversary $\mathcal{A}$ making at most q queries to E finds triples $(k_1, x_1, y_1), \ldots, (k_m, x_m, y_m)$ (with $E_{k_i}(x_i) = y_i$) satisfying $\mathcal{R}$ with probability at most ε.

Example

- consider E in Davies-Meyer mode $f(k, x) := E_k(x) \oplus x$
- finding a preimage of 0 for f is a unary $(q, \mathcal{O}(\frac{q}{2^n}))$-evasive relation for E [BRS02]
- finding a collision for f is a binary $\left(q, \mathcal{O}(\frac{q^2}{2^n})\right)$-evasive relation for E [BRS02]
- for BC-based hashing, most hash function security notions can be recast as evasive relations for the underlying BC

Formalizing Chosen-Key Attacks

Definition (Evasive relation)

An m-ary relation $\mathcal{R}$ is (q, ε)-evasive (w.r.t. an ideal cipher E) if any adversary $\mathcal{A}$ making at most q queries to E finds triples $(k_1, x_1, y_1), \ldots,$ (k_m, x_m, y_m) (with $E_{k_i}(x_i) = y_i$) satisfying $\mathcal{R}$ with probability at most ε.

Example

- consider E in Davies-Meyer mode $f(k, x) := E_k(x) \oplus x$
- finding a preimage of 0 for f is a unary $(q, \mathcal{O}(\frac{q}{2^n}))$-evasive relation for E [BRS02]
- finding a collision for f is a binary $\left(q, \mathcal{O}(\frac{q^2}{2^n})\right)$-evasive relation for E [BRS02]
- for BC-based hashing, most hash function security notions can be recast as evasive relations for the underlying BC

Formalizing Chosen-Key Attacks

Definition (Correlation Intractability)

A block cipher construction $\mathcal{C}^F$ based on some underlying primitive F is said to be (q, ε)-correlation intractable w.r.t. an m-ary relation $\mathcal{R}$ if any adversary $\mathcal{A}$ making at most q queries to F finds triples $(k_1, x_1, y_1), \ldots,$ (k_m, x_m, y_m) (with $\mathcal{C}^F_{k_i}(x_i) = y_i$) satisfying $\mathcal{R}$ with probability at most ε.

Definition (Resistance to Chosen-Key Attacks)

Informally, a block cipher construction $\mathcal{C}^F$ is said resistant to chosen-key attacks if for any (q, ε)-evasive relation $\mathcal{R}$, $\mathcal{C}^F$ is (q', ε')-correlation intractable w.r.t. $\mathcal{R}$ with $q' \simeq q$ and $\varepsilon' \simeq \varepsilon$.

Formalizing Chosen-Key Attacks

Definition (Correlation Intractability)

A block cipher construction $\mathcal{C}^F$ based on some underlying primitive F is said to be (q, ε)-correlation intractable w.r.t. an m-ary relation $\mathcal{R}$ if any adversary $\mathcal{A}$ making at most q queries to F finds triples $(k_1, x_1, y_1), \ldots,$ (k_m, x_m, y_m) (with $\mathcal{C}^F_{k_i}(x_i) = y_i$) satisfying $\mathcal{R}$ with probability at most ε.

Definition (Resistance to Chosen-Key Attacks)

Informally, a block cipher construction $\mathcal{C}^F$ is said resistant to chosen-key attacks if for any (q, ε)-evasive relation $\mathcal{R}$, $\mathcal{C}^F$ is (q', ε')-correlation intractable w.r.t. $\mathcal{R}$ with $q' \simeq q$ and $\varepsilon' \simeq \varepsilon$.

Formalizing Chosen-Key Attacks

Definition (Correlation Intractability)

A block cipher construction $\mathcal{C}^F$ based on some underlying primitive F is said to be (q, ε)-correlation intractable w.r.t. an m tion $\mathcal{R}$ if any adversary $\mathcal{A}$ making at most q queries t $, x_1, y_1), \ldots,$ (k_m, x_m, y_m) (with $\mathcal{C}^F_{k_i}(x_i) = y_i$ at most ε.

Definition (R cks)

Informal uction $\mathcal{C}^F$ is said resistant to chosen-key attacks i $\varepsilon)$-evasive relation $\mathcal{R}$, $\mathcal{C}^F$ is (q', ε')-correlation intractabl w.r.t. $\mathcal{R}$ with $q' \simeq q$ and $\varepsilon' \simeq \varepsilon$.

For any relation $\mathcal{R}$, finding triplets $(\mathsf{k_i}, \mathsf{x_i}, \mathsf{y_i})$ satisfying $\mathcal{R}$ should be "almost as hard" for the construction $\mathcal{C}^F$ as for an ideal cipher.

Formalizing Chosen-Key Attacks

How do we prove prove resistance to chosen-key attacks?

- we use a weaker variant of indifferentiability called sequential indifferentiability
- 12 rounds provide full indifferentiability [LS13] which implies sequential indifferentiability
- is it possible to reduce the number of rounds to get resistance to chosen-key attacks?

Formalizing Chosen-Key Attacks

How do we prove prove resistance to chosen-key attacks?

- we use a weaker variant of indifferentiability called sequential indifferentiability
- 12 rounds provide full indifferentiability [LS13] which implies sequential indifferentiability
- is it possible to reduce the number of rounds to get resistance to chosen-key attacks?

Formalizing Chosen-Key Attacks

How do we prove prove resistance to chosen-key attacks?

- we use a weaker variant of indifferentiability called sequential indifferentiability
- 12 rounds provide full indifferentiability [LS13] which implies sequential indifferentiability
- is it possible to reduce the number of rounds to get resistance to chosen-key attacks?

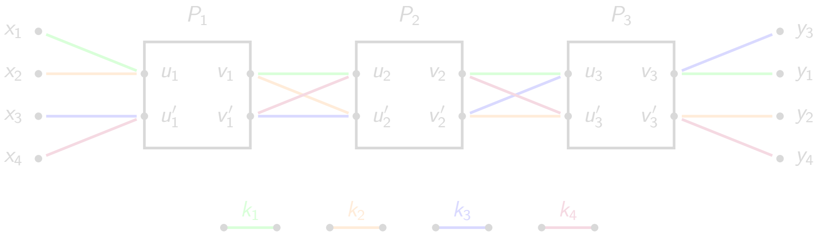
Formalizing Chosen-Key Attacks

How do we prove prove resistance to chosen-key attacks?

- we use a weaker variant of indifferentiability called sequential indifferentiability
- 12 rounds provide full indifferentiability [LS13] which implies sequential indifferentiability
- is it possible to reduce the number of rounds to get resistance to chosen-key attacks?

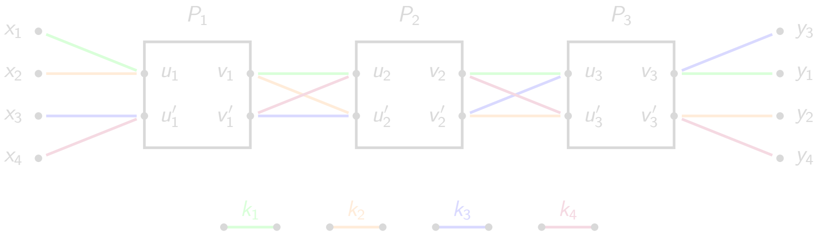
Formalizing Chosen-Key Attacks

3 rounds are not enough [LS13]



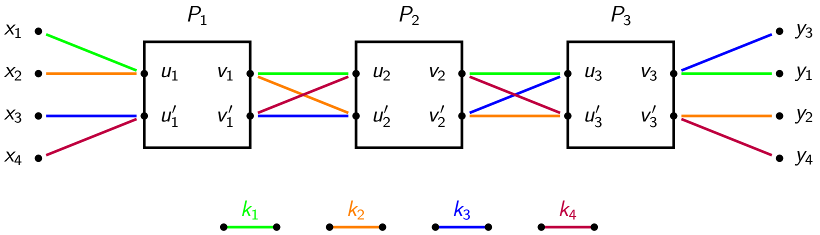
Formalizing Chosen-Key Attacks

3 rounds are not enough [LS13]



Formalizing Chosen-Key Attacks

3 rounds are not enough [LS13]



CKA Resistance for the 4-Round IEM Cipher

Theorem

Let $\mathcal{R}$ be a $(q^2, \varepsilon_{\mathrm{ic}})$-evasive relation w.r.t. an ideal cipher. Then the 4-round IEM with the trivial key-schedule is $\left(q, \varepsilon_{\mathrm{ic}} + \mathcal{O}(\frac{q^4}{2^n})\right)$ correlation intractable w.r.t. $\mathcal{R}$.

Example

Consider f = 4-round IEM cipher in Davies-Meyer mode. Then

- f is $\left(q, \mathcal{O}(\frac{q^4}{2^n})\right)$-preimage resistant
- f is $\left(q, \mathcal{O}(\frac{q^4}{2^n})\right)$-collision resistant

(in the Random Permutation Model)

CKA Resistance for the 4-Round IEM Cipher

Theorem

Let $\mathcal{R}$ be a $(q^2, \varepsilon_{\mathrm{ic}})$-evasive relation w.r.t. an ideal cipher. Then the 4-round IEM with the trivial key-schedule is $\left(q, \varepsilon_{\mathrm{ic}} + \mathcal{O}(\frac{q^4}{2^n})\right)$ correlation intractable w.r.t. $\mathcal{R}$.

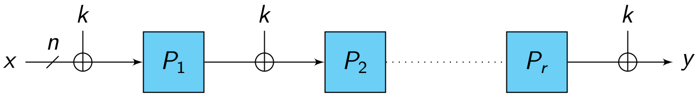
Example

Consider f = 4-round IEM cipher in Davies-Meyer mode. Then

- f is $\left(q, \mathcal{O}(\frac{q^4}{2^n})\right)$-preimage resistant
- f is $\left(q, \mathcal{O}(\frac{q^4}{2^n})\right)$-collision resistant

(in the Random Permutation Model)

Conclusion



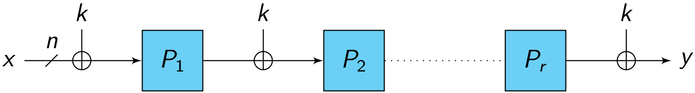
1 round: PRP

3 rounds: XOR-Related-Key-Attacks PRP

4 rounds: Chosen-Key-Attacks Resistance

12 rounds: Full indifferentiability from an ideal cipher

Conclusion



1 round: PRP

3 rounds: XOR-Related-Key-Attacks PRP

4 rounds: Chosen-Key-Attacks Resistance

12 rounds: Full indifferentiability from an ideal cipher

Conclusion

Morality:

- idealized models can be fruitful
- practical meaning of the results is debatable:
  - the high-level structure of SPNs is sound (and may even yield something close to an ideal cipher)
  - says little about concrete block ciphers (inner permutations of, say, AES are too simple)

Open problems:

- RKA security beyond the birthday bound (4 rounds → $2^{\frac{2n}{3}}$-security?)
- a matching $\mathrm{xor\text{-}rka}$ in $\mathcal{O}(2^{\frac{n}{2}})$ queries against 3 rounds

Conclusion

Morality:

- idealized models can be fruitful
- practical meaning of the results is debatable:
  - the high-level structure of SPNs is sound (and may even yield something close to an ideal cipher)
  - says little about concrete block ciphers (inner permutations of, say, AES are too simple)

Open problems:

- RKA security beyond the birthday bound (4 rounds → $2^{\frac{2n}{3}}$-security?)
- a matching $\mathrm{xor\text{-}rka}$ in $\mathcal{O}(2^{\frac{n}{2}})$ queries against 3 rounds

Conclusion

Morality:

- idealized models can be fruitful
- practical meaning of the results is debatable:
  - the high-level structure of SPNs is sound (and may even yield something close to an ideal cipher)
  - says little about concrete block ciphers (inner permutations of, say, AES are too simple)

Open problems:

- RKA security beyond the birthday bound (4 rounds → $2^{\frac{2n}{3}}$-security?)
- a matching $\mathrm{xor\text{-}rka}$ in $\mathcal{O}(2^{\frac{n}{2}})$ queries against 3 rounds

Conclusion

Morality:

- idealized models can be fruitful
- practical meaning of the results is debatable:
  - the high-level structure of SPNs is sound (and may even yield something close to an ideal cipher)
  - says little about concrete block ciphers (inner permutations of, say, AES are too simple)

Open problems:

- RKA security beyond the birthday bound (4 rounds → $2^{\frac{2n}{3}}$-security?)
- a matching $\mathrm{xor\text{-}rka}$ in $\mathcal{O}(2^{\frac{n}{2}})$ queries against 3 rounds

The End. . .

Thanks for your attention!

Comments or questions?

References I

- Mihir Bellare and Tadayoshi Kohno. A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 491–506. Springer, 2003.

- John Black, Phillip Rogaway, and Thomas Shrimpton. Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *LNCS*, pages 320–335. Springer, 2002.

- Ran Canetti, Oded Goldreich, and Shai Halevi. The Random Oracle Methodology, Revisited (Preliminary Version). In *Symposium on Theory of Computing - STOC '98*, pages 209–218. ACM, 1998. Full version available at `http://arxiv.org/abs/cs.CR/0010019`.

- 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 *LNCS*, pages 327–350. Springer, 2014. Full version available at `http://eprint.iacr.org/2013/222`.

References II

Benoît Cogliati and Yannick Seurin. On the Provable Security of the Iterated Even-Mansour Cipher against Related-Key and Chosen-Key Attacks. In *EUROCRYPT 2015*, 2015. To appear. Full version available at `http://eprint.iacr.org/2015/069`.

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 *LNCS*, pages 336–354. Springer, 2012.

Pooya Farshim and Gordon Procter. The Related-Key Security of Iterated Even-Mansour Ciphers. In *Fast Software Encryption - FSE 2015*, 2015. To appear. Full version available at `http://eprint.iacr.org/2014/953`.

Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. Tweaks and Keys for Block Ciphers: The TWEAKEY Framework. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - Proceedings, Part II*, volume 8874 of *LNCS*, pages 274–288. Springer, 2014.

References III

- Pierre Karpman. From Related-Key Distinguishers to Related-Key-Recovery on Even-Mansour Constructions. ePrint Archive, Report 2015/134, 2015. Available at http://eprint.iacr.org/2015/134.pdf.

- Joe Kilian and Phillip Rogaway. How to Protect DES Against Exhaustive Key Search (an Analysis of DESX). *Journal of Cryptology*, 14(1):17–35, 2001.

- Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable Block Ciphers. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *LNCS*, pages 31–46. Springer, 2002.

- Rodolphe Lampe and Yannick Seurin. How to Construct an Ideal Cipher from a Small Set of Public Permutations. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 (Proceedings, Part I)*, volume 8269 of *LNCS*, pages 444–463. Springer, 2013. Full version available at http://eprint.iacr.org/2013/255.