Security Analysis of Key-Alternating Ciphers in the Even-Mansour Model

Yannick Seurin

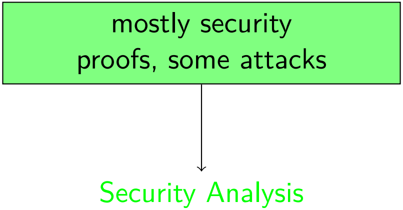
ANSSI

March 20, 2015 — CCA Seminar

The Title

Security Analysis

The Title



The Title

mostly security
proofs, some attacks

↓

Security Analysis of Key-Alternating Ciphers

The Title

mostly security proofs, some attacks

a special class of block ciphers containing most SPN designs (AES, SERPENT, LED, etc.)

↓ ↓

Security Analysis of Key-Alternating Ciphers

The Title

mostly security proofs, some attacks

a special class of block ciphers containing most SPN designs (AES, SERPENT, LED, etc.)

Security Analysis of Key-Alternating Ciphers

in the Even-Mansour Model

The Title

mostly security proofs, some attacks

a special class of block ciphers containing most SPN designs (AES, SERPENT, LED, etc.)

Security Analysis of Key-Alternating Ciphers

in the Even-Mansour Model

a generic model where some internal components of BCs are modeled as public random oracles

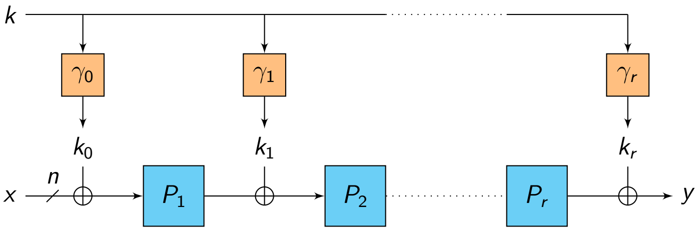
Talk Mainly Based on Joint Work with:

- Jacques Patarin (Versailles Univ.)
- Rodolphe Lampe (Versailles Univ.)
- Benoît Cogliati (Versailles Univ.)
- Jooyoung Lee (Sejong Univ.)
- John Steinberger (Tsinghua Univ.)
- Shan Chen (Tsinghua Univ.)

Outline

Outline

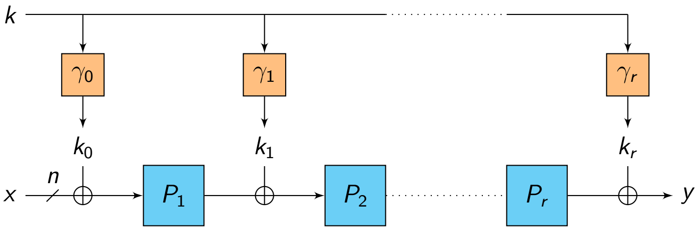
Key-Alternating Cipher (KAC): Definition



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 γ_i's are key derivation functions mapping k to n-bit "round keys"
- examples: most SPNs (AES, SERPENT, PRESENT, LED, ...)

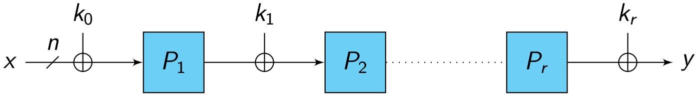
Key-Alternating Cipher (KAC): Definition



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 γ_i's are key derivation functions mapping k to n-bit "round keys"
- examples: most SPNs (AES, SERPENT, PRESENT, LED, ...)

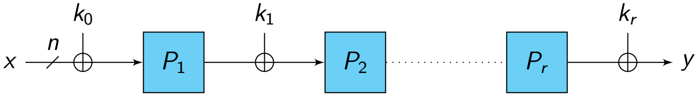
Various Key-Schedule Types



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: $(\gamma_0(k), \gamma_1(k), \ldots, \gamma_r(k))$
- 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)

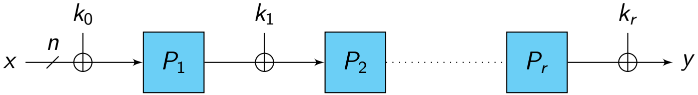
Various Key-Schedule Types



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: $(\gamma_0(k), \gamma_1(k), \ldots, \gamma_r(k))$
- 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)

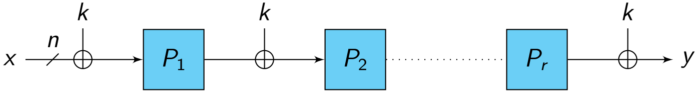
Various Key-Schedule Types



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: $(\gamma_0(k), \gamma_1(k), \ldots, \gamma_r(k))$
- 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)

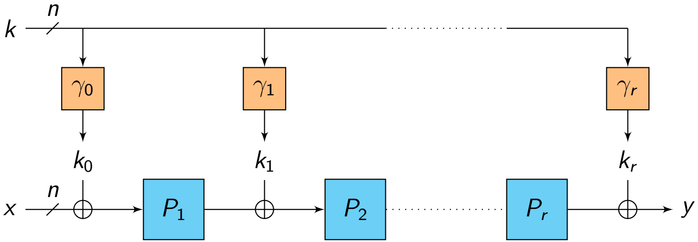
Various Key-Schedule Types



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: $(\gamma_0(k), \gamma_1(k), \ldots, \gamma_r(k))$
- 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)

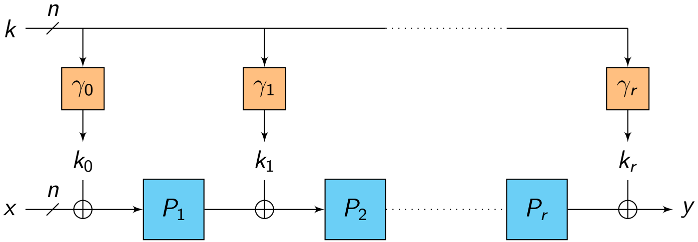
Various Key-Schedule Types



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: $(\gamma_0(k), \gamma_1(k), \ldots, \gamma_r(k))$
- 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)

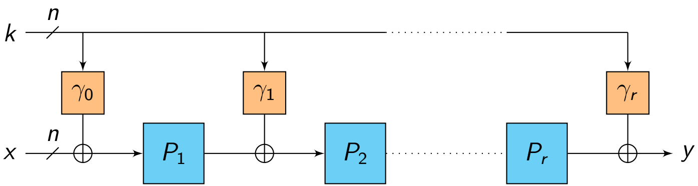
Various Key-Schedule Types



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: $(\gamma_0(k), \gamma_1(k), \ldots, \gamma_r(k))$
- 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

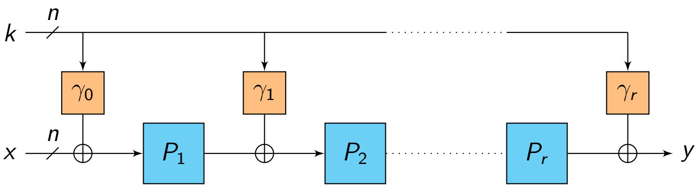


Question

How can we "prove" security?

- against a general adversary:
  $\Rightarrow$ 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

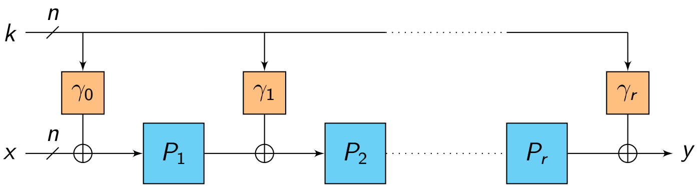


Question

How can we “prove” security?

- against a general adversary:
  $\Rightarrow$ 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

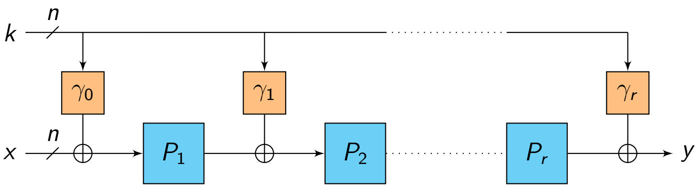


Question

How can we "prove" security?

- against a general adversary:
  $\Rightarrow$ 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

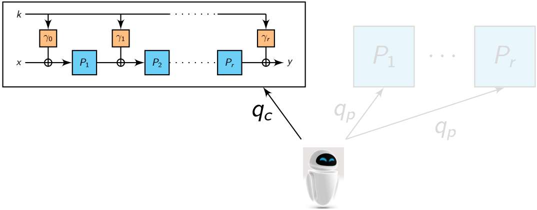


Question

How can we "prove" security?

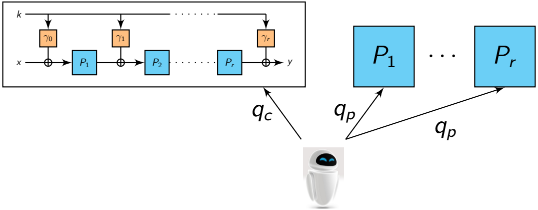
- against a general adversary:
  $\Rightarrow$ too hard (unconditional complexity lower bound!)
- against specific attacks (differential, linear. . .):
  $\Rightarrow$ use specific design of $P_1, \ldots, P_r$ (count active S-boxes, etc.)
- against generic attacks:
  $\Rightarrow$ Random Permutation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

Analyzing KACs in the Random Permutation Model



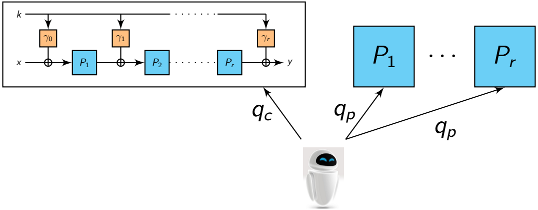
- the P_i's are modeled as public random permutation oracles to which the adversary can only make black-box queries (both to P_i and P_i^{-1})
- adversary cannot exploit any weakness of the P_i's $\Rightarrow$ generic attacks
- trades complexity for randomness ($\simeq$ Random Oracle Model)
- complexity 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



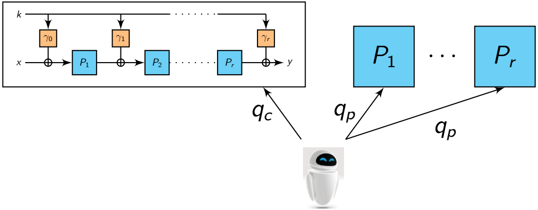
- the P_i's are modeled as public random permutation oracles to which the adversary can only make black-box queries (both to P_i and P_i^{-1})
- adversary cannot exploit any weakness of the P_i's $\Rightarrow$ generic attacks
- trades complexity for randomness ($\simeq$ Random Oracle Model)
- complexity 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



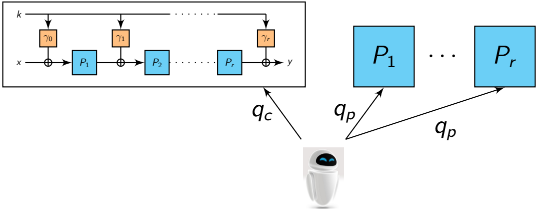
- the P_i's are modeled as public random permutation oracles to which the adversary can only make black-box queries (both to P_i and P_i^{-1})
- adversary cannot exploit any weakness of the P_i's $\Rightarrow$ generic attacks
- trades complexity for randomness ($\simeq$ Random Oracle Model)
- complexity 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



- 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



- 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

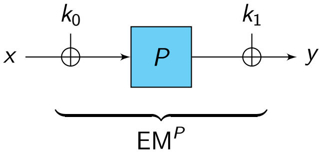
Even and Mansour seminal work:

- 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 secure up to $\mathcal{O}(2^{\frac{n}{2}})$ queries of the adversary to P and to the cipher
- similar result when $k_0 = k_1$ [DKS12]

Analyzing KACs in the Random Permutation Model

Even and Mansour seminal work:

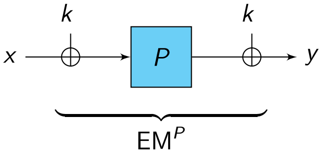
- this model was first proposed by Even and Mansour at ASIACRYPT '91 for $r = 1$ round
- they showed that the simple cipher $k_1 \oplus P(k_0 \oplus x)$ is secure up to $\mathcal{O}(2^{\frac{n}{2}})$ queries of the adversary to P and to the cipher
- similar result when $k_0 = k_1$ [DKS12]



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 secure up to $\mathcal{O}(2^{\frac{n}{2}})$ queries of the adversary to P and to the cipher
- similar result when $k_0 = k_1$ [DKS12]



A Word on Wording

Even-Mansour Model
=
Random Permutation Model

"the" Iterated Even-Mansour (IEM) Cipher
=
generic class of key-alternating ciphers
analyzed in the Random Permutation Model

A Word on Wording

Even-Mansour Model
=
Random Permutation Model

"the" Iterated Even-Mansour (IEM) Cipher
=
generic class of key-alternating ciphers
analyzed in the Random Permutation Model

20 Years After

Revival of the approach:

- basically not much progress after ASIACRYPT '91 until...
- EUROCRYPT 2012 paper by Bogdanov *et al.*
- they showed that for $r = 2$ the security bound is pushed back to $\mathcal{O}(2^{\frac{2n}{3}})$ adversarial queries
- triggered a spate of results
  (at least 10 proof papers + 6 cryptanalysis papers)
- Why 20 years?
  - the model is far from actual designs ("simple" inner permutations)
  - cryptanalysts not interested in generic attacks on BCs
    (until publication of LED, PRINCE, etc.)

20 Years After

Revival of the approach:

- basically not much progress after ASIACRYPT '91 until...
- EUROCRYPT 2012 paper by Bogdanov *et al.*
- they showed that for $r = 2$ the security bound is pushed back to $\mathcal{O}(2^{\frac{2n}{3}})$ adversarial queries
- triggered a spate of results
  (at least 10 proof papers + 6 cryptanalysis papers)
- Why 20 years?
  - the model is far from actual designs ("simple" inner permutations)
  - cryptanalysts not interested in generic attacks on BCs
    (until publication of LED, PRINCE, etc.)

20 Years After

Revival of the approach:

- basically not much progress after ASIACRYPT '91 until...
- EUROCRYPT 2012 paper by Bogdanov *et al.*
- they showed that for $r = 2$ the security bound is pushed back to $\mathcal{O}(2^{\frac{2n}{3}})$ adversarial queries
- triggered a spate of results
  (at least 10 proof papers + 6 cryptanalysis papers)
- Why 20 years?
  - the model is far from actual designs ("simple" inner permutations)
  - cryptanalysts not interested in generic attacks on BCs
    (until publication of LED, PRINCE, etc.)

20 Years After

Revival of the approach:

- basically not much progress after ASIACRYPT '91 until...
- EUROCRYPT 2012 paper by Bogdanov *et al.*
- they showed that for $r = 2$ the security bound is pushed back to $\mathcal{O}(2^{\frac{2n}{3}})$ adversarial queries
- triggered a spate of results (at least 10 proof papers + 6 cryptanalysis papers)
- Why 20 years?
  - the model is far from actual designs ("simple" inner permutations)
  - cryptanalysts not interested in generic attacks on BCs (until publication of LED, PRINCE, etc.)

20 Years After

Revival of the approach:

- basically not much progress after ASIACRYPT '91 until...
- EUROCRYPT 2012 paper by Bogdanov *et al.*
- they showed that for $r = 2$ the security bound is pushed back to $\mathcal{O}(2^{\frac{2n}{3}})$ adversarial queries
- triggered a spate of results (at least 10 proof papers + 6 cryptanalysis papers)
- Why 20 years?
  - the model is far from actual designs ("simple" inner permutations)
  - cryptanalysts not interested in generic attacks on BCs (until publication of LED, PRINCE, etc.)

20 Years After

Revival of the approach:

- basically not much progress after ASIACRYPT '91 until...
- EUROCRYPT 2012 paper by Bogdanov *et al.*
- they showed that for $r = 2$ the security bound is pushed back to $\mathcal{O}(2^{\frac{2n}{3}})$ adversarial queries
- triggered a spate of results
  (at least 10 proof papers + 6 cryptanalysis papers)
- Why 20 years?
  - the model is far from actual designs ("simple" inner permutations)
  - cryptanalysts not interested in generic attacks on BCs
    (until publication of LED, PRINCE, etc.)

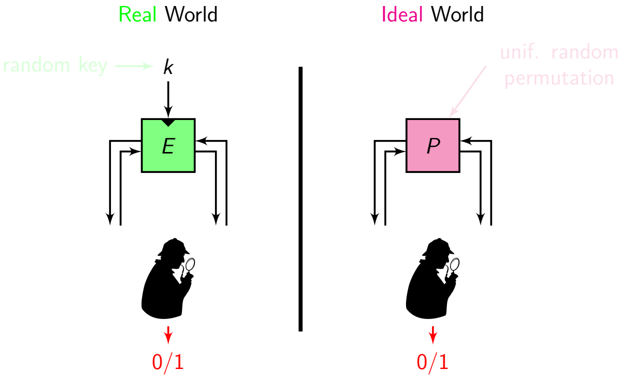
20 Years After

Revival of the approach:

- basically not much progress after ASIACRYPT '91 until...
- EUROCRYPT 2012 paper by Bogdanov *et al.*
- they showed that for $r = 2$ the security bound is pushed back to $\mathcal{O}(2^{\frac{2n}{3}})$ adversarial queries
- triggered a spate of results
  (at least 10 proof papers + 6 cryptanalysis papers)
- Why 20 years?
  - the model is far from actual designs ("simple" inner permutations)
  - cryptanalysts not interested in generic attacks on BCs
    (until publication of LED, PRINCE, etc.)

Outline

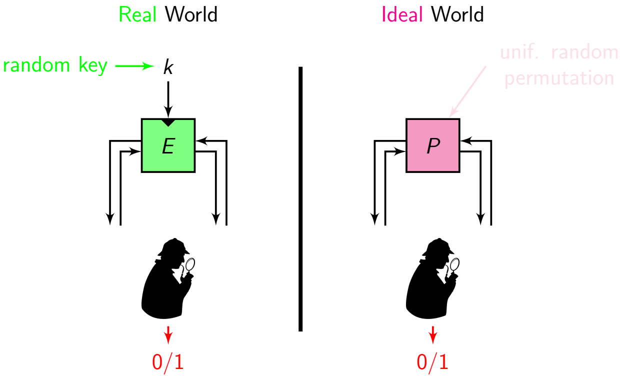
Formalizing Block Cipher Security: Pseudorandomness



SPRP (*a.k.a.* CCA) advantage:

$$\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{D}) = \left| \Pr\left[\mathcal{D}^{E_k} = 1\right] - \Pr\left[\mathcal{D}^{P} = 1\right] \right|$$

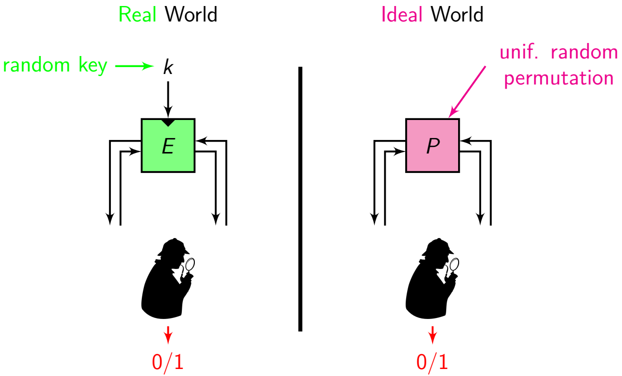
Formalizing Block Cipher Security: Pseudorandomness



SPRP (*a.k.a.* CCA) advantage:

$$\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{D}) = \left|\Pr\left[\mathcal{D}^{E_k} = 1\right] - \Pr\left[\mathcal{D}^{P} = 1\right]\right|$$

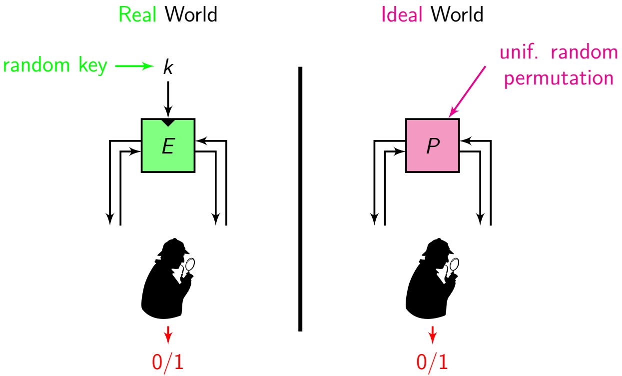
Formalizing Block Cipher Security: Pseudorandomness



SPRP (*a.k.a.* CCA) advantage:

$$\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{D}) = \left| \Pr\left[\mathcal{D}^{E_k} = 1\right] - \Pr\left[\mathcal{D}^{P} = 1\right] \right|$$

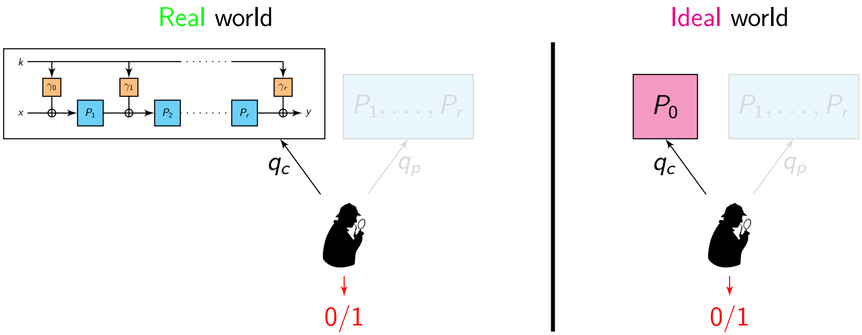
Formalizing Block Cipher Security: Pseudorandomness



SPRP (*a.k.a.* CCA) advantage:

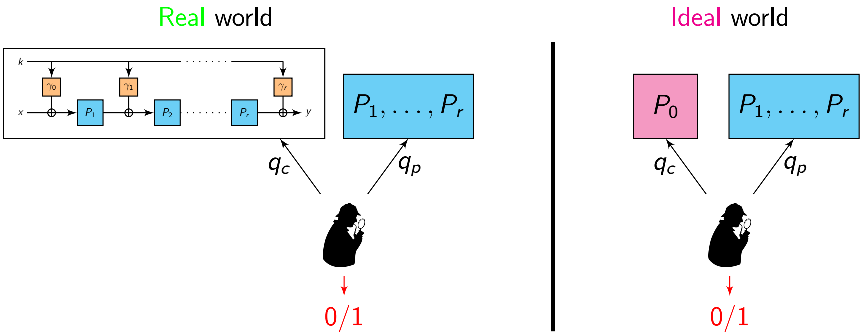
$$\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{D}) = \left| \Pr\left[\mathcal{D}^{E_k} = 1\right] - \Pr\left[\mathcal{D}^{P} = 1\right] \right|$$

Formalizing Pseudorandomness for the IEM Cipher



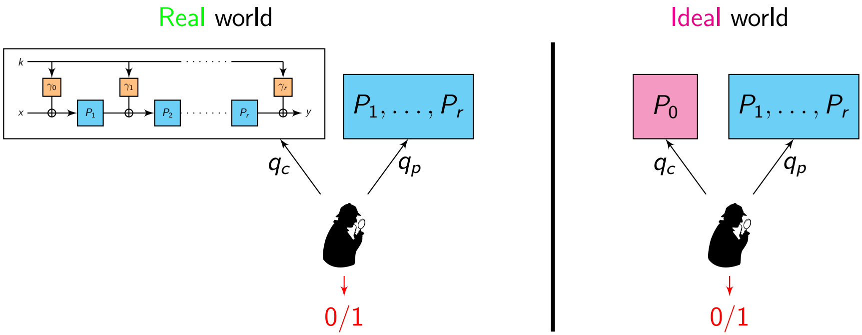
- real world: IEM cipher with a random key $k \leftarrow_{\$} \{0,1\}^{\kappa}$
- ideal world: random permutation P_0 independent from $P_1, \ldots, P_r$
- Rand. Perm. Model: $\mathcal{D}$ has oracle access to $P_1, \ldots, P_r$ in both worlds
- q_c queries to the IEM/P_0 and q_p queries to each inner perm.

Formalizing Pseudorandomness for the IEM Cipher



- real world: IEM cipher with a random key $k \leftarrow_{\$} \{0,1\}^{\kappa}$
- ideal world: random permutation P_0 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/P_0 and q_p queries to each inner perm.

Formalizing Pseudorandomness for the IEM Cipher



- real world: IEM cipher with a random key $k \leftarrow_\$ \{0,1\}^\kappa$
- ideal world: random permutation P_0 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/P_0 and q_p queries to each inner perm.

Pseudorandomness of the IEM Cipher: Main Result

Theorem (Chen-Steinberger [CS14])

For independent round keys $(k_0, \ldots, k_r)$ and independent inner permutations $P_1, \ldots, P_r$, the best distinguishing advantage against the r-round IEM cipher satisfies

$$\mathbf{Adv}^{\mathrm{sprp}}_{\mathsf{EM}[n,r]}(q_c, q_p) \leq \mathcal{O}\left(\frac{q_c q_p^r}{2^{rn}}\right)$$

- holds when the $r+1$ round keys are only r-wise independent, e.g.

$$(k_0, k_0 \oplus k_1, k_1 \oplus k_2, \ldots, k_{r-1} \oplus k_r, k_r)$$

- often shortened to "secure up to $\mathcal{O}(2^{\frac{rn}{r+1}})$ queries" by letting $q_{\mathrm{tot}} = q_c + rq_p$
- the result is tight (matched by exhaustive key-search, see later)

Pseudorandomness of the IEM Cipher: Main Result

Theorem (Chen-Steinberger [CS14])

For independent round keys $(k_0, \ldots, k_r)$ *and independent inner permutations* $P_1, \ldots, P_r$*, the best distinguishing advantage against the* r*-round IEM cipher satisfies*

$$\mathbf{Adv}^{\mathrm{sprp}}_{\mathsf{EM}[n,r]}(q_c, q_p) \leq \mathcal{O}\left(\frac{q_c q_p^r}{2^{rn}}\right)$$

- holds when the $r+1$ round keys are only r-wise independent, e.g.

$$(k_0, k_0 \oplus k_1, k_1 \oplus k_2, \ldots, k_{r-1} \oplus k_r, k_r)$$

- often shortened to "secure up to $\mathcal{O}(2^{\frac{rn}{r+1}})$ queries" by letting $q_{\mathrm{tot}} = q_c + rq_p$
- the result is tight (matched by exhaustive key-search, see later)

Pseudorandomness of the IEM Cipher: Main Result

Theorem (Chen-Steinberger [CS14])

For independent round keys $(k_0, \ldots, k_r)$ and independent inner permutations $P_1, \ldots, P_r$, the best distinguishing advantage against the r-round IEM cipher satisfies

$$\mathbf{Adv}^{\mathrm{sprp}}_{\mathsf{EM}[n,r]}(q_c, q_p) \leq \mathcal{O}\left(\frac{q_c q_p^r}{2^{rn}}\right) = \mathcal{O}\left(\frac{q_{\mathrm{tot}}^{r+1}}{2^{rn}}\right)$$

- holds when the $r+1$ round keys are only r-wise independent, e.g.

$$(k_0, k_0 \oplus k_1, k_1 \oplus k_2, \ldots, k_{r-1} \oplus k_r, k_r)$$

- often shortened to "secure up to $\mathcal{O}(2^{\frac{rn}{r+1}})$ queries" by letting $q_{\mathrm{tot}} = q_c + rq_p$
- the result is tight (matched by exhaustive key-search, see later)

Pseudorandomness of the IEM Cipher: Main Result

Theorem (Chen-Steinberger [CS14])

For independent round keys $(k_0, \ldots, k_r)$ *and independent inner permutations* $P_1, \ldots, P_r$*, the best distinguishing advantage against the* r*-round IEM cipher satisfies*

$$\mathbf{Adv}^{\mathrm{sprp}}_{\mathsf{EM}[n,r]}(q_c, q_p) \leq \mathcal{O}\left(\frac{q_c q_p^r}{2^{rn}}\right) = \mathcal{O}\left(\frac{q_{\mathrm{tot}}^{r+1}}{2^{rn}}\right)$$

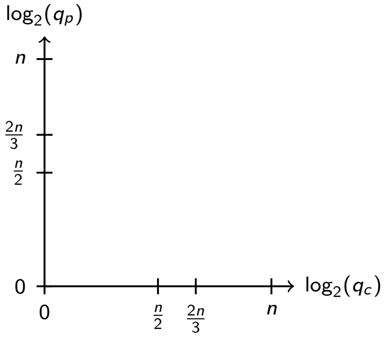
- holds when the $r+1$ round keys are only r-wise independent, e.g.

$$(k_0, k_0 \oplus k_1, k_1 \oplus k_2, \ldots, k_{r-1} \oplus k_r, k_r)$$

- often shortened to "secure up to $\mathcal{O}(2^{\frac{rn}{r+1}})$ queries" by letting $q_{\mathrm{tot}} = q_c + rq_p$
- the result is tight (matched by exhaustive key-search, see later)

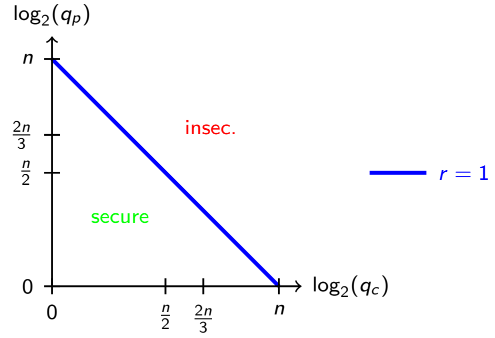
Pseudorandomness of the IEM Cipher: Main Result

Plotting the bound in the plan (q_c, q_p):



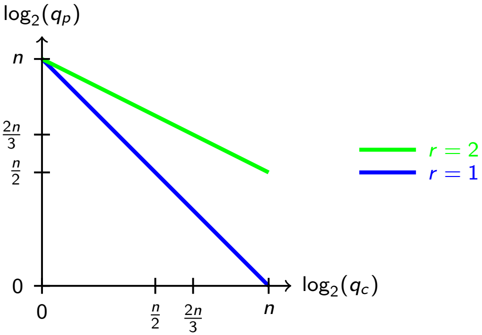
Pseudorandomness of the IEM Cipher: Main Result

Plotting the bound in the plan (q_c, q_p):



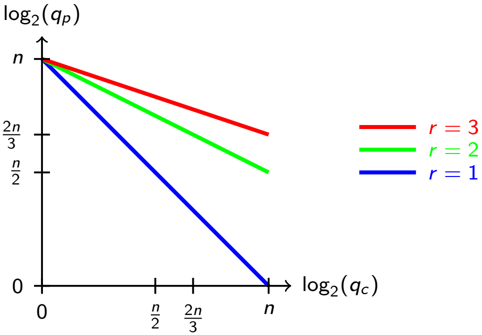
Pseudorandomness of the IEM Cipher: Main Result

Plotting the bound in the plan (q_c, q_p):



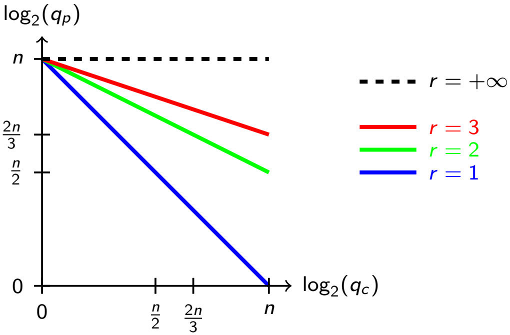
Pseudorandomness of the IEM Cipher: Main Result

Plotting the bound in the plan (q_c, q_p):



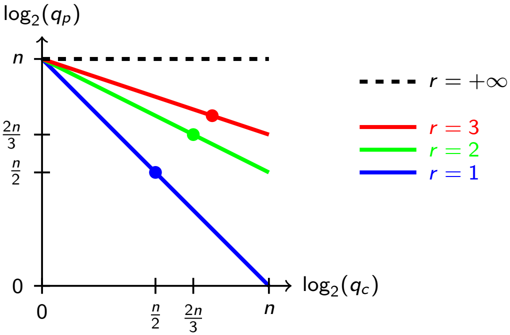
Pseudorandomness of the IEM Cipher: Main Result

Plotting the bound in the plan (q_c, q_p):



Pseudorandomness of the IEM Cipher: Main Result

Plotting the bound in the plan (q_c, q_p):



Pseudorandomness of the IEM Cipher: History

[CS14] closed the following series of work:

- tight bound for $r = 1$: Even-Mansour [EM97] (proof: game-based)
- tight bound for $r = 2$: Bogdanov *et al.* [BKL+12] (proof: game-based, intricate!)
- tight bound for $r = 3$: Steinberger [Ste12] (proof: Hellinger distance)
- non-tight bound $\mathcal{O}(2^{\frac{rn}{r+2}})$ for any even r: Lampe-Patarin-Seurin [LPS12] (proof: coupling technique)
- tight bound for any r: Chen-Steinberger [CS14] (proof: H-coefficients technique)

Pseudorandomness of the IEM Cipher: History

[CS14] closed the following series of work:

- tight bound for $r = 1$: Even-Mansour [EM97] (proof: game-based)
- tight bound for $r = 2$: Bogdanov *et al.* [BKL+12] (proof: game-based, intricate!)
- tight bound for $r = 3$: Steinberger [Ste12] (proof: Hellinger distance)
- non-tight bound $\mathcal{O}(2^{\frac{rn}{r+2}})$ for any even r: Lampe-Patarin-Seurin [LPS12] (proof: coupling technique)
- tight bound for any r: Chen-Steinberger [CS14] (proof: H-coefficients technique)

Pseudorandomness of the IEM Cipher: History

[CS14] closed the following series of work:

- tight bound for $r = 1$: Even-Mansour [EM97] (proof: game-based)
- tight bound for $r = 2$: Bogdanov *et al.* [BKL+12] (proof: game-based, intricate!)
- tight bound for $r = 3$: Steinberger [Ste12] (proof: Hellinger distance)
- non-tight bound $\mathcal{O}(2^{\frac{rn}{r+2}})$ for any even r: Lampe-Patarin-Seurin [LPS12] (proof: coupling technique)
- tight bound for any r: Chen-Steinberger [CS14] (proof: H-coefficients technique)

Pseudorandomness of the IEM Cipher: History

[CS14] closed the following series of work:

- tight bound for $r = 1$: Even-Mansour [EM97] (proof: game-based)
- tight bound for $r = 2$: Bogdanov *et al.* [BKL+12] (proof: game-based, intricate!)
- tight bound for $r = 3$: Steinberger [Ste12] (proof: Hellinger distance)
- non-tight bound $\mathcal{O}(2^{\frac{rn}{r+2}})$ for any even r: Lampe-Patarin-Seurin [LPS12] (proof: coupling technique)
- tight bound for any r: Chen-Steinberger [CS14] (proof: H-coefficients technique)

Pseudorandomness of the IEM Cipher: History

[CS14] closed the following series of work:

- tight bound for $r = 1$: Even-Mansour [EM97] (proof: game-based)
- tight bound for $r = 2$: Bogdanov *et al.* [BKL$^+$12] (proof: game-based, intricate!)
- tight bound for $r = 3$: Steinberger [Ste12] (proof: Hellinger distance)
- non-tight bound $\mathcal{O}(2^{\frac{rn}{r+2}})$ for any even r: Lampe-Patarin-Seurin [LPS12] (proof: coupling technique)
- tight bound for any r: Chen-Steinberger [CS14] (proof: H-coefficients technique)

A Cautionary Note on Attacks

Matching attack:

- there is a matching attack with $q_c, q_p \simeq 2^{\frac{rn}{r+1}}$: exhaustive key-search!
- in other words: exhaustive key-search does not require to make the 2^n possible queries to the P_i's!
- but this is still exhaustive key-search: time $2^\kappa \geq 2^n$!
- exceptions (for independent round keys):
  - $r = 1$ round: Daemen's attack [Dae91], time $t \simeq 2^{\frac{n}{2}}$
  - $r = 2$ rounds: Dinur *et al.* attack [DDKS13], time $t \simeq 2^{n - \log n} > 2^{\frac{2n}{3}}$
- for $r \geq 3$, best attack requires $t \simeq 2^{(r+1)n}$

A Cautionary Note on Attacks

Matching attack:

- there is a matching attack with $q_c, q_p \simeq 2^{\frac{rn}{r+1}}$: exhaustive key-search!
- in other words: exhaustive key-search does not require to make the 2^n possible queries to the P_i's!
- but this is still exhaustive key-search: time $2^\kappa \geq 2^n$!
- exceptions (for independent round keys):
  - $r = 1$ round: Daemen's attack [Dae91], time $t \simeq 2^{\frac{n}{2}}$
  - $r = 2$ rounds: Dinur *et al.* attack [DDKS13], time $t \simeq 2^{n-\log n} > 2^{\frac{2n}{3}}$
- for $r \geq 3$, best attack requires $t \simeq 2^{(r+1)n}$

A Cautionary Note on Attacks

Matching attack:

- there is a matching attack with $q_c, q_p \simeq 2^{\frac{rn}{r+1}}$: exhaustive key-search!
- in other words: exhaustive key-search does not require to make the 2^n possible queries to the P_i's!
- but this is still exhaustive key-search: time $2^\kappa \geq 2^n$!
- exceptions (for independent round keys):
  - $r = 1$ round: Daemen's attack [Dae91], time $t \simeq 2^{\frac{n}{2}}$
  - $r = 2$ rounds: Dinur *et al.* attack [DDKS13], time $t \simeq 2^{n - \log n} > 2^{\frac{2n}{3}}$
- for $r \geq 3$, best attack requires $t \simeq 2^{(r+1)n}$

A Cautionary Note on Attacks

Matching attack:

- there is a matching attack with $q_c, q_p \simeq 2^{\frac{rn}{r+1}}$: exhaustive key-search!
- in other words: exhaustive key-search does not require to make the 2^n possible queries to the P_i's!
- but this is still exhaustive key-search: time $2^\kappa \geq 2^n$!
- exceptions (for independent round keys):
  - $r = 1$ round: Daemen's attack [Dae91], time $t \simeq 2^{\frac{n}{2}}$
  - $r = 2$ rounds: Dinur *et al.* attack [DDKS13], time $t \simeq 2^{n - \log n} > 2^{\frac{2n}{3}}$
- for $r \geq 3$, best attack requires $t \simeq 2^{(r+1)n}$

A Cautionary Note on Attacks

Matching attack:

- there is a matching attack with $q_c, q_p \simeq 2^{\frac{rn}{r+1}}$: exhaustive key-search!
- in other words: exhaustive key-search does not require to make the 2^n possible queries to the P_i's!
- but this is still exhaustive key-search: time $2^\kappa \geq 2^n$!
- exceptions (for independent round keys):
  - $r = 1$ round: Daemen's attack [Dae91], time $t \simeq 2^{\frac{n}{2}}$
  - $r = 2$ rounds: Dinur *et al.* attack [DDKS13], time $t \simeq 2^{n - \log n} > 2^{\frac{2n}{3}}$
- for $r \geq 3$, best attack requires $t \simeq 2^{(r+1)n}$

A Cautionary Note on Attacks

Matching attack:

- there is a matching attack with $q_c, q_p \simeq 2^{\frac{rn}{r+1}}$: exhaustive key-search!
- in other words: exhaustive key-search does not require to make the 2^n possible queries to the P_i's!
- but this is still exhaustive key-search: time $2^\kappa \geq 2^n$!
- exceptions (for independent round keys):
  - $r = 1$ round: Daemen's attack [Dae91], time $t \simeq 2^{\frac{n}{2}}$
  - $r = 2$ rounds: Dinur *et al.* attack [DDKS13], time $t \simeq 2^{n - \log n} > 2^{\frac{2n}{3}}$
- for $r \geq 3$, best attack requires $t \simeq 2^{(r+1)n}$

A Cautionary Note on Attacks

Matching attack:

- there is a matching attack with $q_c, q_p \simeq 2^{\frac{rn}{r+1}}$: exhaustive key-search!
- in other words: exhaustive key-search does not require to make the 2^n possible queries to the P_i's!
- but this is still exhaustive key-search: time $2^\kappa \geq 2^n$!
- exceptions (for independent round keys):
  - $r = 1$ round: Daemen's attack [Dae91], time $t \simeq 2^{\frac{n}{2}}$
  - $r = 2$ rounds: Dinur *et al.* attack [DDKS13], time $t \simeq 2^{n-\log n} > 2^{\frac{2n}{3}}$
- for $r \geq 3$, best attack requires $t \simeq 2^{(r+1)n}$

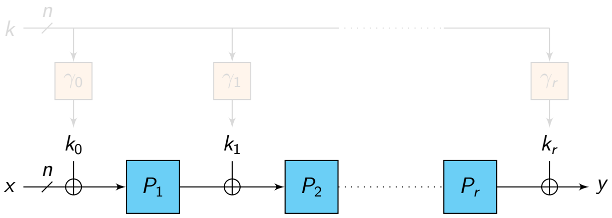
Reducing the Key-Length and the Number of Permutations

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, etc.)?



Positive answer for $r = 2$ rounds: $\mathcal{O}(2^{\frac{2n}{3}})$-security bound [CLL+14]

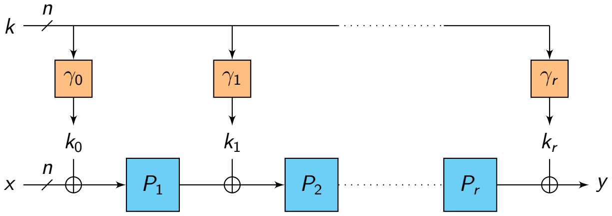
Reducing the Key-Length and the Number of Permutations

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, etc.)?



Positive answer for $r = 2$ rounds: $\mathcal{O}(2^{\frac{2n}{3}})$-security bound [CLL+14]

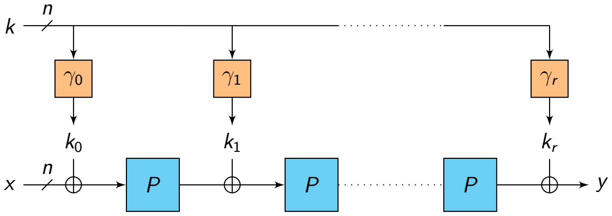
Reducing the Key-Length and the Number of Permutations

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, etc.)?



Positive answer for $r = 2$ rounds: $\mathcal{O}(2^{\frac{2n}{3}})$-security bound [CLL+14]

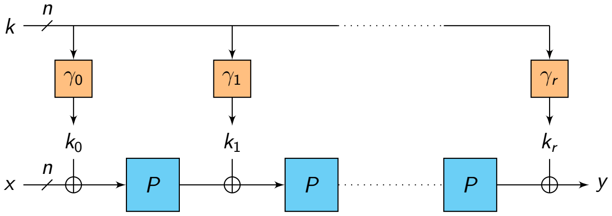
Reducing the Key-Length and the Number of Permutations

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, etc.)?



Positive answer for $r = 2$ rounds: $\mathcal{O}(2^{\frac{2n}{3}})$-security bound [CLL+14]

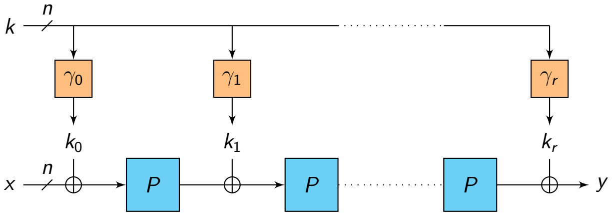
Reducing the Key-Length and the Number of Permutations

Question:

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

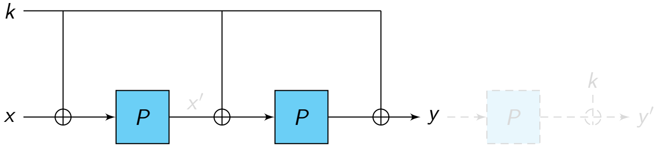
- the round keys $(k_0, \ldots, k_r)$ are derived from an *n*-bit master key
- and/or when the same permutation P is used at each round

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



Positive answer for $r = 2$ rounds: $\mathcal{O}(2^{\frac{2n}{3}})$-security bound [CLL+14]

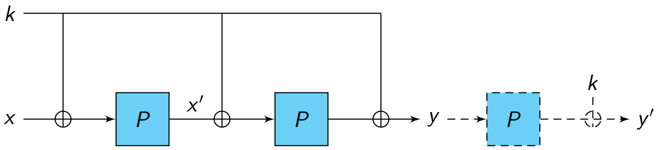
A Non-Trivial Key-Schedule is Necessary



Slide Attack for Identical Permutations and Trivial KS:

- find $(x, y), (x', y')$ such that $x' = P(x \oplus k)$ (slid pair)
- can be detected by checking that $x \oplus P(y) = y' \oplus P^{-1}(x')$
- requires $\sim \mathcal{O}(2^{\frac{n}{2}})$ queries to E and P by the birthday paradox
- works for any number of rounds

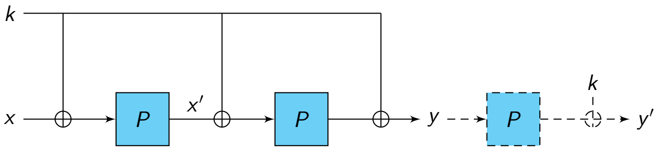
A Non-Trivial Key-Schedule is Necessary



Slide Attack for Identical Permutations and Trivial KS:

- find $(x, y), (x', y')$ such that $x' = P(x \oplus k)$ (slid pair)
- can be detected by checking that $x \oplus P(y) = y' \oplus P^{-1}(x')$
- requires $\sim \mathcal{O}(2^{\frac{n}{2}})$ queries to E and P by the birthday paradox
- works for any number of rounds

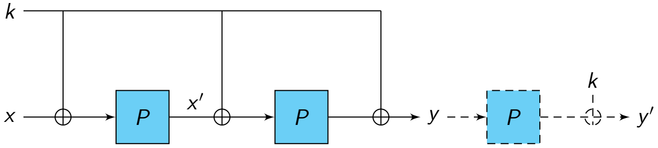
A Non-Trivial Key-Schedule is Necessary



Slide Attack for Identical Permutations and Trivial KS:

- find $(x, y), (x', y')$ such that $x' = P(x \oplus k)$ (slid pair)
- can be detected by checking that $x \oplus P(y) = y' \oplus P^{-1}(x')$
- requires $\sim \mathcal{O}(2^{\frac{n}{2}})$ queries to E and P by the birthday paradox
- works for any number of rounds

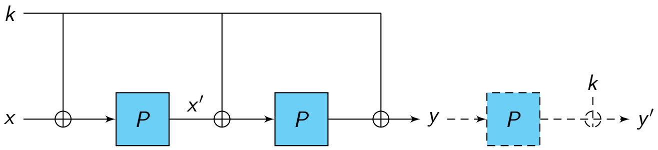
A Non-Trivial Key-Schedule is Necessary



Slide Attack for Identical Permutations and Trivial KS:

- find $(x, y), (x', y')$ such that $x' = P(x \oplus k)$ (slid pair)
- can be detected by checking that $x \oplus P(y) = y' \oplus P^{-1}(x')$
- requires $\sim \mathcal{O}(2^{\frac{n}{2}})$ queries to E and P by the birthday paradox
- works for any number of rounds

A Non-Trivial Key-Schedule is Necessary



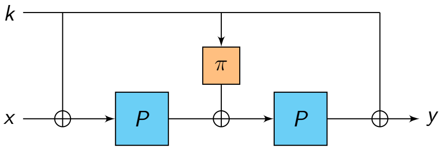
Slide Attack for Identical Permutations and Trivial KS:

- find $(x, y), (x', y')$ such that $x' = P(x \oplus k)$ (slid pair)
- can be detected by checking that $x \oplus P(y) = y' \oplus P^{-1}(x')$
- requires $\sim \mathcal{O}(2^{\frac{n}{2}})$ queries to E and P by the birthday paradox
- works for any number of rounds

Provably Secure Construction for 2 Rounds

Theorem (Chen *et al.* [CLL+14])

The IEM 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

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

Outline

Introduction and History

Pseudorandomness of Key-Alternating Ciphers

Beyond Pseudorandomness: Related-Key Attacks

Beyond RKAs: Chosen-Key Attacks and Indifferentiability

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

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

- NB: independent work by Farshim and Procter at FSE 2015 [FP15]

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

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

- NB: independent work by Farshim and Procter at FSE 2015 [FP15]

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

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

- NB: independent work by Farshim and Procter at FSE 2015 [FP15]

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

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

- NB: independent work by Farshim and Procter at FSE 2015 [FP15]

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

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

- NB: independent work by Farshim and Procter at FSE 2015 [FP15]

Related-Key Attacks

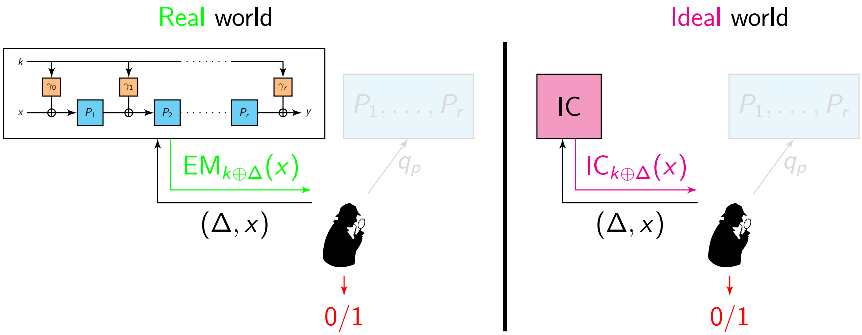
The Related-Key Attack Model [BK03]:

- 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

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

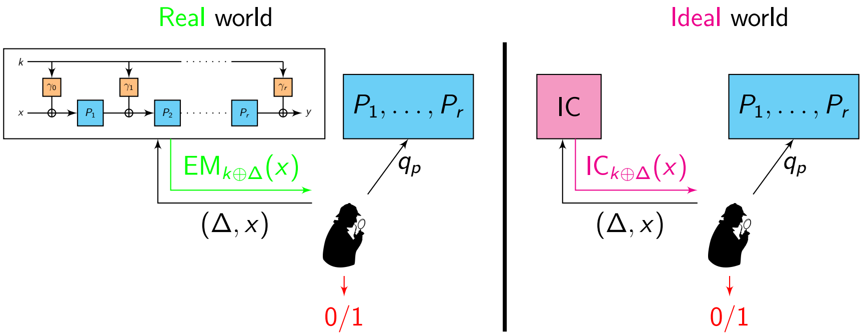
- NB: independent work by Farshim and Procter at FSE 2015 [FP15]

XOR-RKAs against the IEM Cipher: Formalization



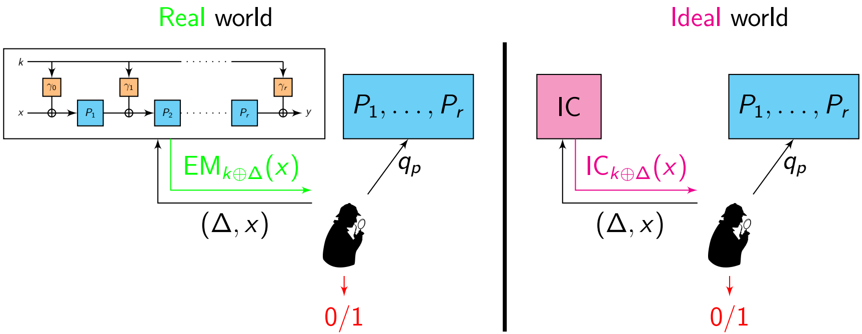
- real world: IEM cipher with a random key $k \leftarrow_{\$} \{0,1\}^{\kappa}$
- ideal world: ideal cipher IC independent from $P_1, \ldots, P_r$
- Rand. Perm. Model: $\mathcal{D}$ has oracle access to $P_1, \ldots, P_r$ in both worlds
- q_c queries to the IEM/IC and q_p queries to each inner perm.

XOR-RKAs against the IEM Cipher: Formalization



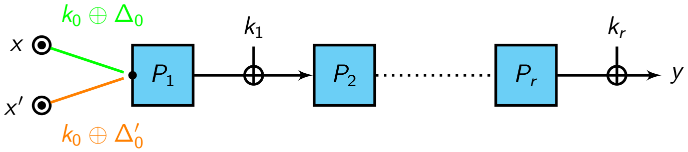
- real world: IEM cipher with a random key $k \leftarrow_\$ \{0,1\}^\kappa$
- ideal world: ideal cipher IC independent from $P_1, \ldots, P_r$
- Rand. Perm. Model: $\mathcal{D}$ has oracle access to $P_1, \ldots, P_r$ in both worlds
- q_c queries to the IEM/IC and q_p queries to each inner perm.

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 $P_1, \ldots, P_r$
- 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



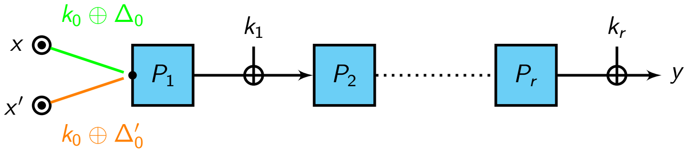
RK Distinguisher for independent round keys:

- 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 round keys derived from an n-bit master key

First Observation: Independent Round Keys Fails



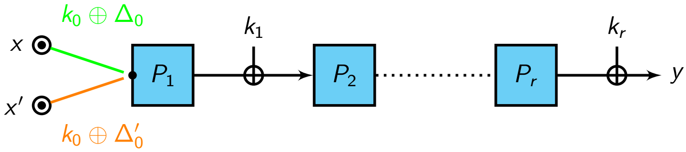
RK Distinguisher for independent round keys:

- 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 round keys derived from an n-bit master key

First Observation: Independent Round Keys Fails



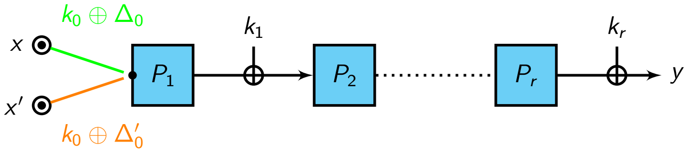
RK Distinguisher for independent round keys:

- 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 round keys derived from an n-bit master key

First Observation: Independent Round Keys Fails



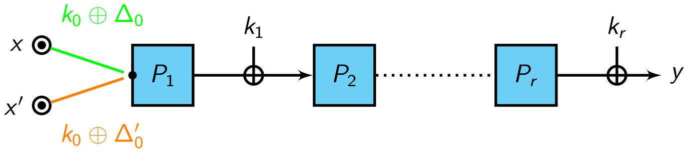
RK Distinguisher for independent round keys:

- 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 round keys derived from an n-bit master key

First Observation: Independent Round Keys Fails



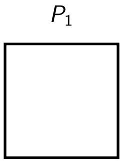
RK Distinguisher for independent round keys:

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

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

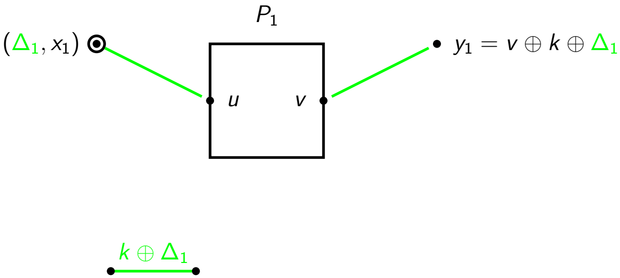
- check that the outputs are equal
- holds with proba. 1 for the IEM cipher
- holds with proba. 2^{-n} for an ideal cipher
- $\Rightarrow$ we will consider round keys derived from an n-bit master key

A Simple Attack for One Round, Trivial Key-Schedule



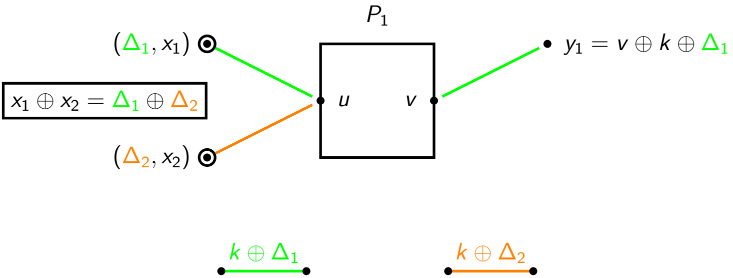
- 2 queries to the RK oracle, 0 queries to P_1
- $(*)$ holds with proba. 1 for the EM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule

A Simple Attack for One Round, Trivial Key-Schedule



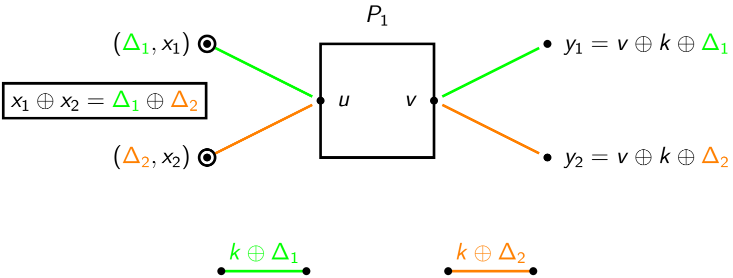
- 2 queries to the RK oracle, 0 queries to P_1
- $(*)$ holds with proba. 1 for the EM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule

A Simple Attack for One Round, Trivial Key-Schedule



- 2 queries to the RK oracle, 0 queries to P_1
- $(*)$ holds with proba. 1 for the EM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule

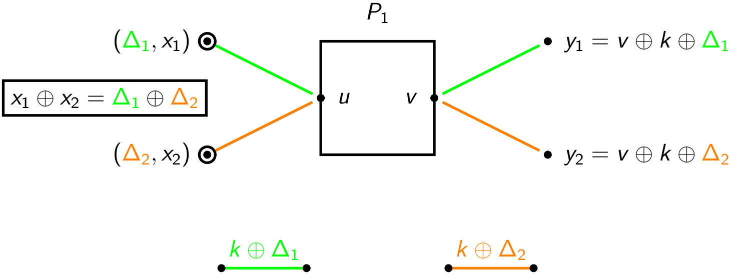
A Simple Attack for One Round, Trivial Key-Schedule



Check that $y_1 \oplus y_2 = \Delta_1 \oplus \Delta_2$ $(*)$

- 2 queries to the RK oracle, 0 queries to P_1
- $(*)$ holds with proba. 1 for the EM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule

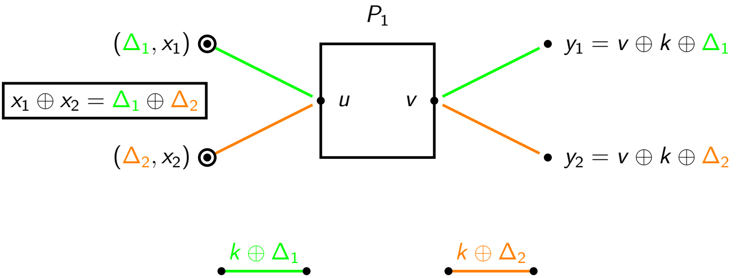
A Simple Attack for One Round, Trivial Key-Schedule



Check that $y_1 \oplus y_2 = \Delta_1 \oplus \Delta_2$ $(*)$

- 2 queries to the RK oracle, 0 queries to P_1
- $(*)$ holds with proba. 1 for the EM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule

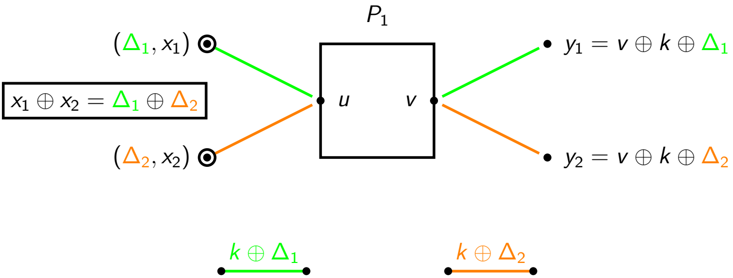
A Simple Attack for One Round, Trivial Key-Schedule



Check that $y_1 \oplus y_2 = \Delta_1 \oplus \Delta_2$ $(*)$

- 2 queries to the RK oracle, 0 queries to P_1
- $(*)$ holds with proba. 1 for the EM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule

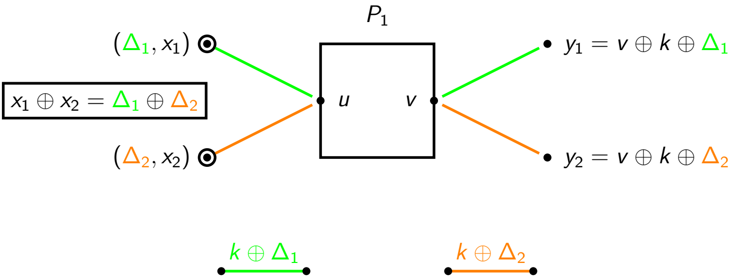
A Simple Attack for One Round, Trivial Key-Schedule



Check that $y_1 \oplus y_2 = \Delta_1 \oplus \Delta_2$ $(*)$

- 2 queries to the RK oracle, 0 queries to P_1
- $(*)$ holds with proba. 1 for the EM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule

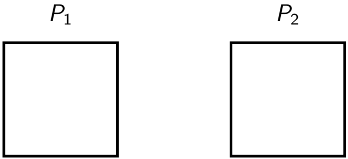
A Simple Attack for One Round, Trivial Key-Schedule



Check that $y_1 \oplus y_2 = \Delta_1 \oplus \Delta_2$ $(*)$

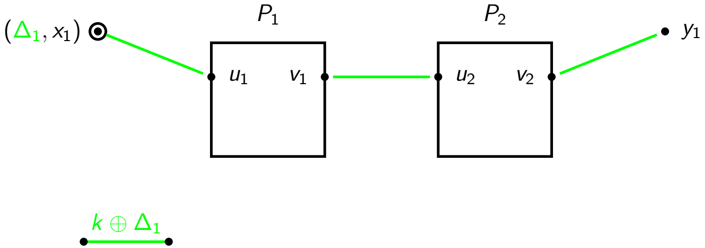
- 2 queries to the RK oracle, 0 queries to P_1
- $(*)$ holds with proba. 1 for the EM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule

An Attack for Two Rounds, Trivial Key-Schedule



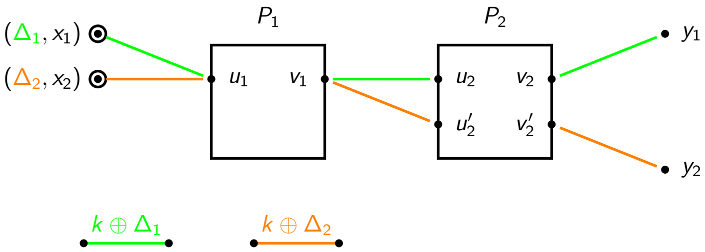
- 4 queries to the RK oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the 2-round IEM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule

An Attack for Two Rounds, Trivial Key-Schedule



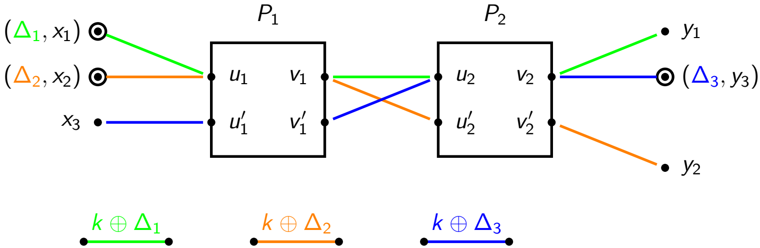
- 4 queries to the RK oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the 2-round IEM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule

An Attack for Two Rounds, Trivial Key-Schedule



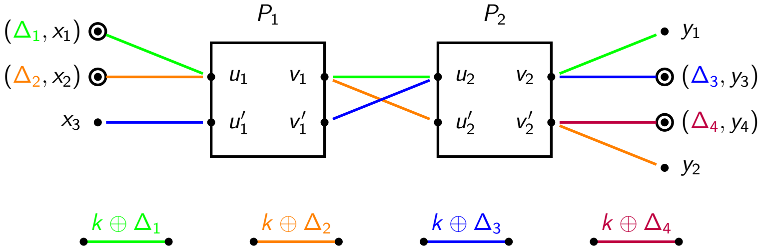
- 4 queries to the RK oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the 2-round IEM cipher
- $(*)$ holds with proba. 2^{-n} for an ideal cipher
- works for any linear key-schedule

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

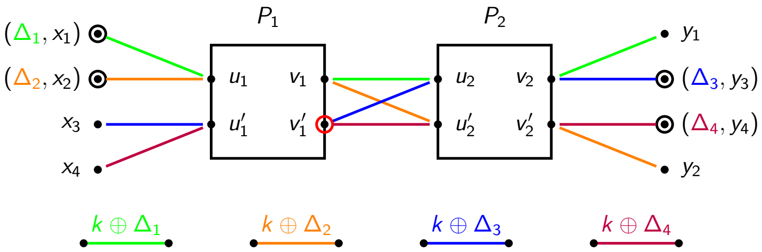
An Attack for Two Rounds, Trivial Key-Schedule



$$\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0$$

- 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

An Attack for Two Rounds, Trivial Key-Schedule

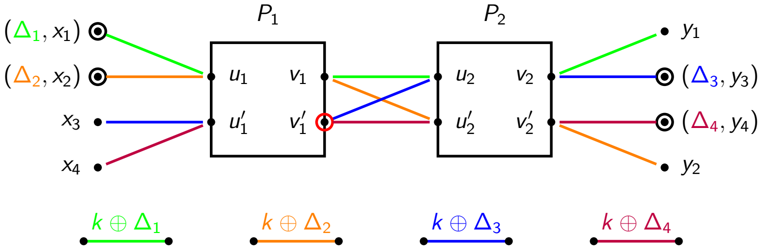


$$\boxed{\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0}$$

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

An Attack for Two Rounds, Trivial Key-Schedule

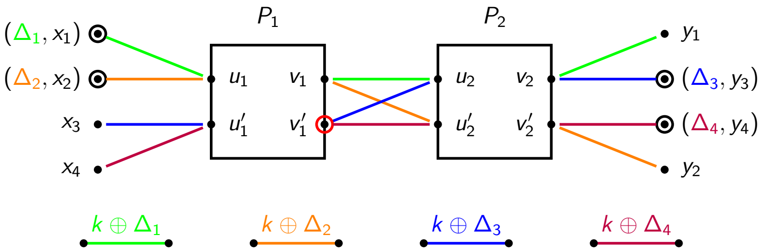


$$\boxed{\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0}$$

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

An Attack for Two Rounds, Trivial Key-Schedule

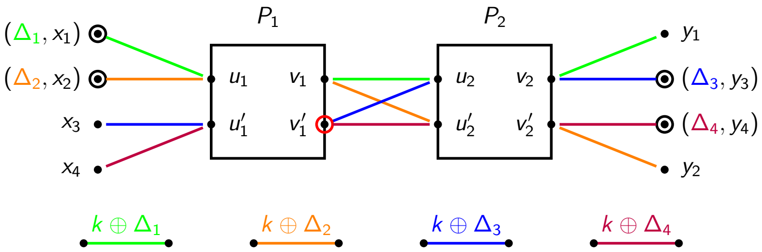


$$\boxed{\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0}$$

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

An Attack for Two Rounds, Trivial Key-Schedule

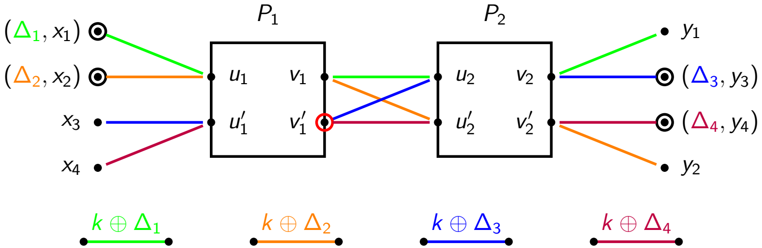


$$\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0$$

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

An Attack for Two Rounds, Trivial Key-Schedule

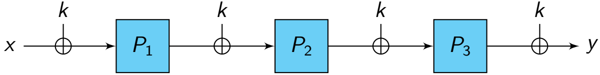


$$\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0$$

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

Security for Three Rounds, Trivial Key-Schedule



Theorem (Cogliati-Seurin [CS15])

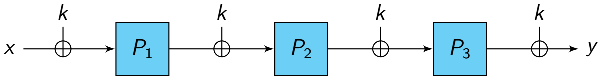
For the 3-round IEM cipher with the trivial key-schedule:

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

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])

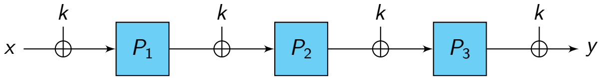
For the 3-round IEM cipher with the trivial key-schedule:

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

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])

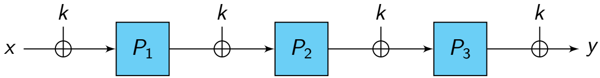
For the 3-round IEM cipher with the trivial key-schedule:

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

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 Three Rounds, Trivial Key-Schedule



Theorem (Cogliati-Seurin [CS15])

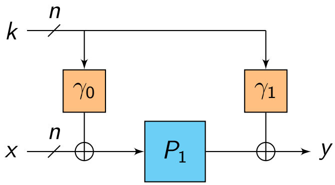
For the 3-round IEM cipher with the trivial key-schedule:

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

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 $\gamma = (\gamma_0, \gamma_1)$*:*

$$\mathbf{Adv}^{\text{xor-rka}}_{\text{EM}[n,1,\gamma]}(q_c, q_p) \leq \frac{2q_c q_p}{2^n} + \frac{(\delta(\gamma_0) + \delta(\gamma_1))q_c^2}{2 \cdot 2^n},$$

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.)*

Outline

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!

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!

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!

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!

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!

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!

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!

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 $\varepsilon' \simeq \varepsilon$.

Questions:

- How do we prove prove resistance to chosen-key attacks?
- How many rounds for the IEM cipher to be resistant to CKAs?

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 $\varepsilon' \simeq \varepsilon$.

Questions:

- How do we prove prove resistance to chosen-key attacks?
- How many rounds for the IEM cipher to be resistant to CKAs?

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 $\varepsilon' \simeq \varepsilon$.

Questions:

- How do we prove prove resistance to chosen-key attacks?
- How many rounds for the IEM cipher to be resistant to CKAs?

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.

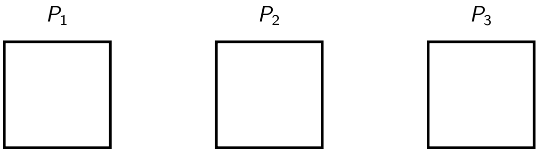
Definition (Resistance to Chosen-Key Attacks)

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 $\varepsilon' \simeq \varepsilon$.

Questions:

- How do we prove prove resistance to chosen-key attacks?
- How many rounds for the IEM cipher to be resistant to CKAs?

A Chosen-Key Attack for Three Rounds [LS13]

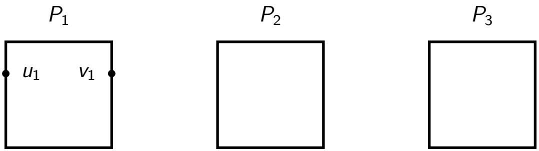


- tuples (k_1, x_1, y_1), (k_2, x_2, y_2), (k_3, x_3, y_3), (k_4, x_4, y_4) satisfy

$$\begin{cases} k_1 \oplus k_2 \oplus k_3 \oplus k_4 = 0 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0 \\ y_1 \oplus y_2 \oplus y_3 \oplus y_4 = 0 \end{cases}.$$

- this is a $\left(q, \mathcal{O}(\frac{q^4}{2^n})\right)$-evasive relation for an ideal cipher
- $\Rightarrow$ the 3-round IEM cipher is not resistant to CKAs

A Chosen-Key Attack for Three Rounds [LS13]

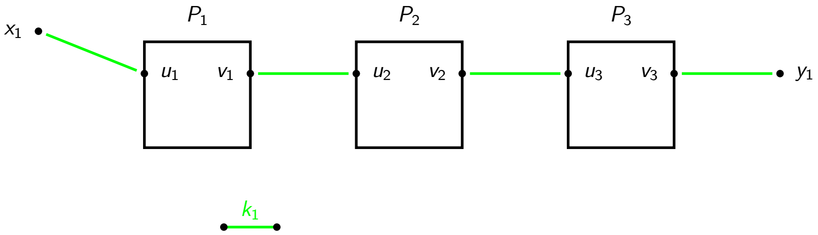


- tuples (k_1, x_1, y_1), (k_2, x_2, y_2), (k_3, x_3, y_3), (k_4, x_4, y_4) satisfy

$$\begin{cases} k_1 \oplus k_2 \oplus k_3 \oplus k_4 = 0 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0 \\ y_1 \oplus y_2 \oplus y_3 \oplus y_4 = 0 \end{cases} .$$

- this is a $\left(q, \mathcal{O}(\frac{q^4}{2^n})\right)$-evasive relation for an ideal cipher
- $\Rightarrow$ the 3-round IEM cipher is not resistant to CKAs

A Chosen-Key Attack for Three Rounds [LS13]

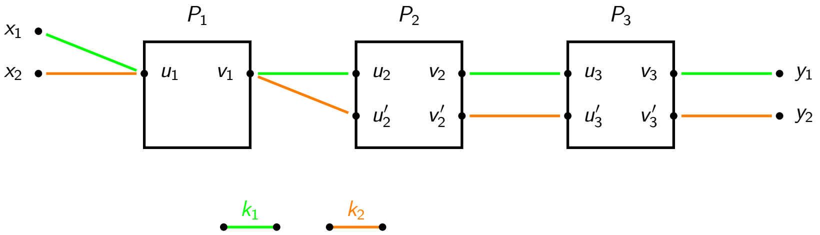


- tuples (k_1, x_1, y_1), (k_2, x_2, y_2), (k_3, x_3, y_3), (k_4, x_4, y_4) satisfy

$$\begin{cases} k_1 \oplus k_2 \oplus k_3 \oplus k_4 = 0 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0 \\ y_1 \oplus y_2 \oplus y_3 \oplus y_4 = 0 \end{cases}.$$

- this is a $\left(q, \mathcal{O}(\frac{q^4}{2^n})\right)$-evasive relation for an ideal cipher
- $\Rightarrow$ the 3-round IEM cipher is not resistant to CKAs

A Chosen-Key Attack for Three Rounds [LS13]

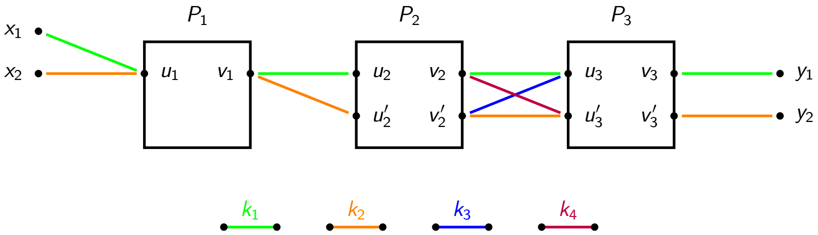


- tuples (k_1, x_1, y_1), (k_2, x_2, y_2), (k_3, x_3, y_3), (k_4, x_4, y_4) satisfy

$$\begin{cases} k_1 \oplus k_2 \oplus k_3 \oplus k_4 = 0 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0 \\ y_1 \oplus y_2 \oplus y_3 \oplus y_4 = 0 \end{cases}.$$

- this is a $\left(q, \mathcal{O}(\frac{q^4}{2^n})\right)$-evasive relation for an ideal cipher
- $\Rightarrow$ the 3-round IEM cipher is not resistant to CKAs

A Chosen-Key Attack for Three Rounds [LS13]

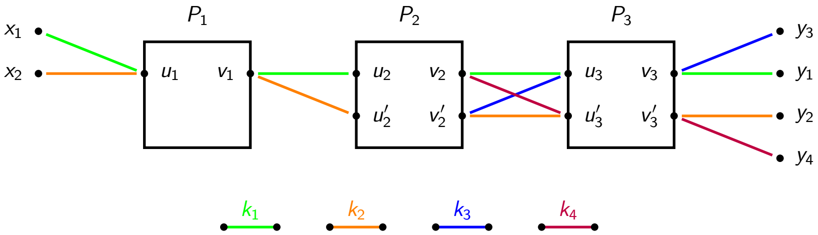


- tuples (k_1, x_1, y_1), (k_2, x_2, y_2), (k_3, x_3, y_3), (k_4, x_4, y_4) satisfy

$$\begin{cases} k_1 \oplus k_2 \oplus k_3 \oplus k_4 = 0 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0 \\ y_1 \oplus y_2 \oplus y_3 \oplus y_4 = 0 \end{cases} .$$

- this is a $\left(q, \mathcal{O}(\frac{q^4}{2^n})\right)$-evasive relation for an ideal cipher
- $\Rightarrow$ the 3-round IEM cipher is not resistant to CKAs

A Chosen-Key Attack for Three Rounds [LS13]

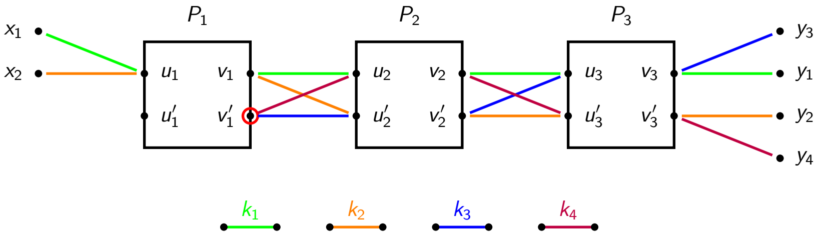


- tuples (k_1, x_1, y_1), (k_2, x_2, y_2), (k_3, x_3, y_3), (k_4, x_4, y_4) satisfy

$$\begin{cases} k_1 \oplus k_2 \oplus k_3 \oplus k_4 = 0 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0 \\ y_1 \oplus y_2 \oplus y_3 \oplus y_4 = 0 \end{cases} .$$

- this is a $\left(q, \mathcal{O}(\frac{q^4}{2^n})\right)$-evasive relation for an ideal cipher
- $\Rightarrow$ the 3-round IEM cipher is not resistant to CKAs

A Chosen-Key Attack for Three Rounds [LS13]

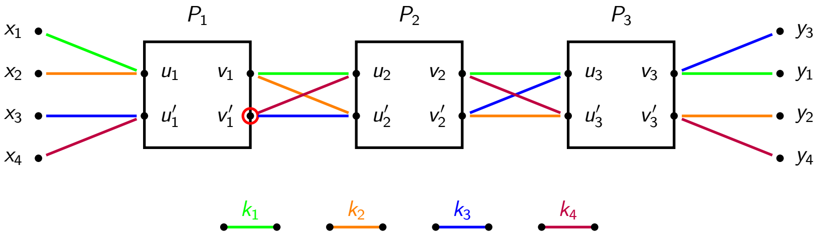


- tuples (k_1, x_1, y_1), (k_2, x_2, y_2), (k_3, x_3, y_3), (k_4, x_4, y_4) satisfy

$$\begin{cases} k_1 \oplus k_2 \oplus k_3 \oplus k_4 = 0 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0 \\ y_1 \oplus y_2 \oplus y_3 \oplus y_4 = 0 \end{cases} .$$

- this is a $\left(q, \mathcal{O}(\frac{q^4}{2^n})\right)$-evasive relation for an ideal cipher
- $\Rightarrow$ the 3-round IEM cipher is not resistant to CKAs

A Chosen-Key Attack for Three Rounds [LS13]

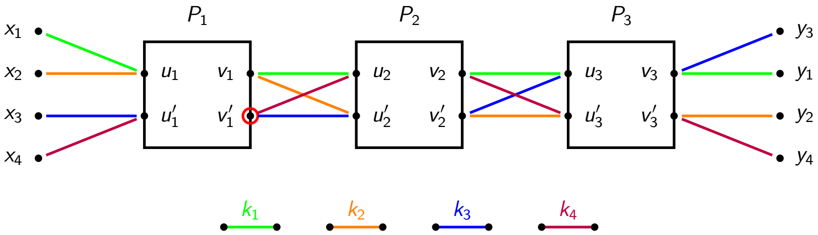


- tuples (k_1, x_1, y_1), (k_2, x_2, y_2), (k_3, x_3, y_3), (k_4, x_4, y_4) satisfy

$$\begin{cases} k_1 \oplus k_2 \oplus k_3 \oplus k_4 = 0 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0 \\ y_1 \oplus y_2 \oplus y_3 \oplus y_4 = 0 \ . \end{cases}$$

- this is a $\left(q, \mathcal{O}(\frac{q^4}{2^n})\right)$-evasive relation for an ideal cipher
- $\Rightarrow$ the 3-round IEM cipher is not resistant to CKAs

A Chosen-Key Attack for Three Rounds [LS13]

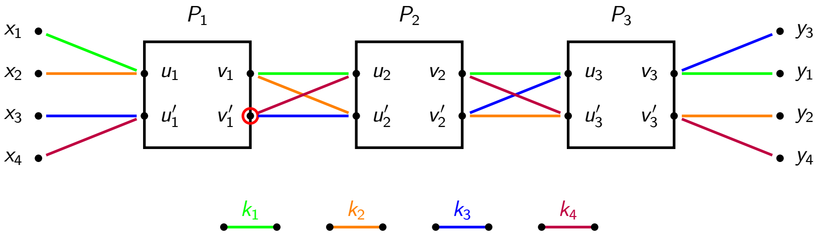


- tuples (k_1, x_1, y_1), (k_2, x_2, y_2), (k_3, x_3, y_3), (k_4, x_4, y_4) satisfy

$$\begin{cases} k_1 \oplus k_2 \oplus k_3 \oplus k_4 = 0 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0 \\ y_1 \oplus y_2 \oplus y_3 \oplus y_4 = 0 \end{cases}.$$

- this is a $\left(q, \mathcal{O}(\frac{q^4}{2^n})\right)$-evasive relation for an ideal cipher
- $\Rightarrow$ the 3-round IEM cipher is not resistant to CKAs

A Chosen-Key Attack for Three Rounds [LS13]

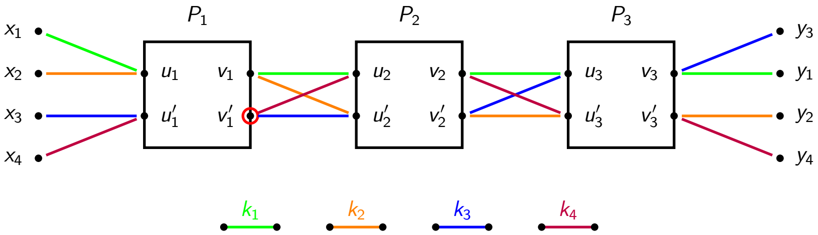


- tuples (k_1, x_1, y_1), (k_2, x_2, y_2), (k_3, x_3, y_3), (k_4, x_4, y_4) satisfy

$$\begin{cases} k_1 \oplus k_2 \oplus k_3 \oplus k_4 = 0 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0 \\ y_1 \oplus y_2 \oplus y_3 \oplus y_4 = 0 \end{cases} .$$

- this is a $\left(q, \mathcal{O}(\frac{q^4}{2^n})\right)$-evasive relation for an ideal cipher
- $\Rightarrow$ the 3-round IEM cipher is not resistant to CKAs

A Chosen-Key Attack for Three Rounds [LS13]

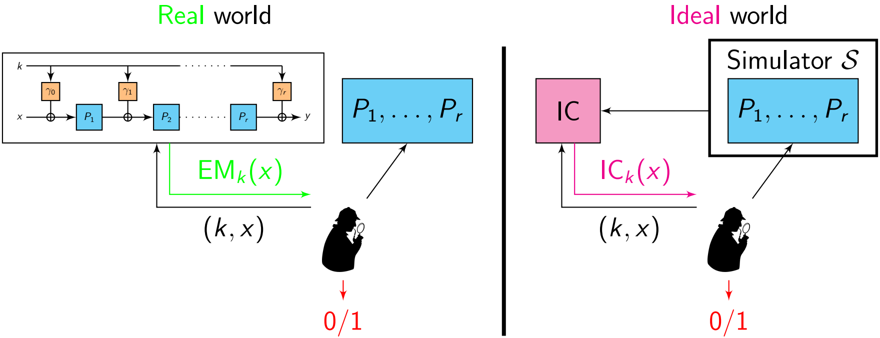


- tuples (k_1, x_1, y_1), (k_2, x_2, y_2), (k_3, x_3, y_3), (k_4, x_4, y_4) satisfy

$$\begin{cases} k_1 \oplus k_2 \oplus k_3 \oplus k_4 = 0 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0 \\ y_1 \oplus y_2 \oplus y_3 \oplus y_4 = 0 \end{cases} .$$

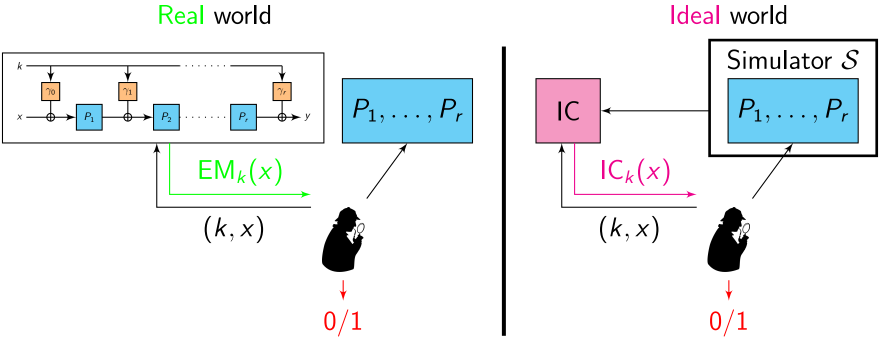
- this is a $\left(q, \mathcal{O}(\frac{q^4}{2^n})\right)$-evasive relation for an ideal cipher
- $\Rightarrow$ the 3-round IEM cipher is not resistant to CKAs

Proving CKA Resistance: Indifferentiability



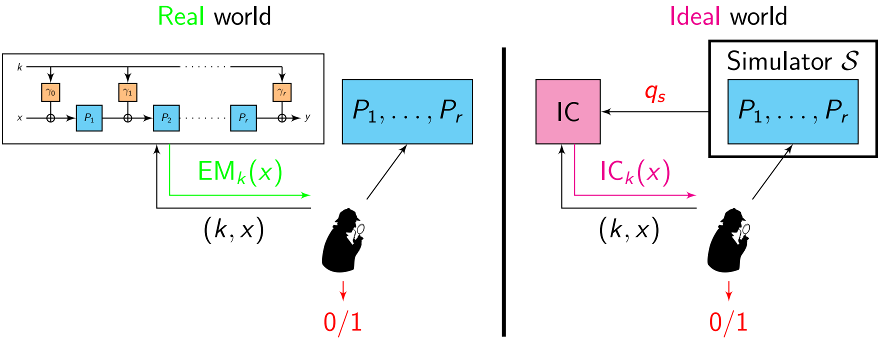
- real world: IEM cipher + random permutations $P_1, \ldots, P_r$
- ideal world: ideal cipher IC + simulator $\mathcal{S}$
- no hidden secret in the real world!
  (but $\mathcal{D}$ can only make a limited number of queries)

Proving CKA Resistance: Indifferentiability



- real world: IEM cipher + random permutations $P_1, \ldots, P_r$
- ideal world: ideal cipher IC + simulator $\mathcal{S}$
- no hidden secret in the real world!
  (but $\mathcal{D}$ can only make a limited number of queries)

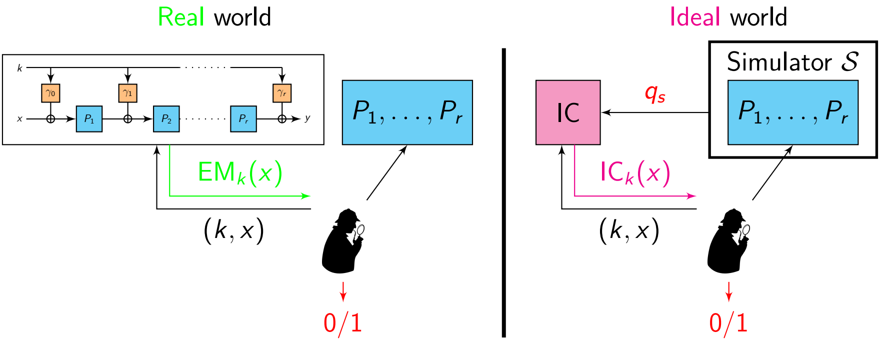
Proving CKA Resistance: Indifferentiability



Definition (Indifferentiability [MRH04])

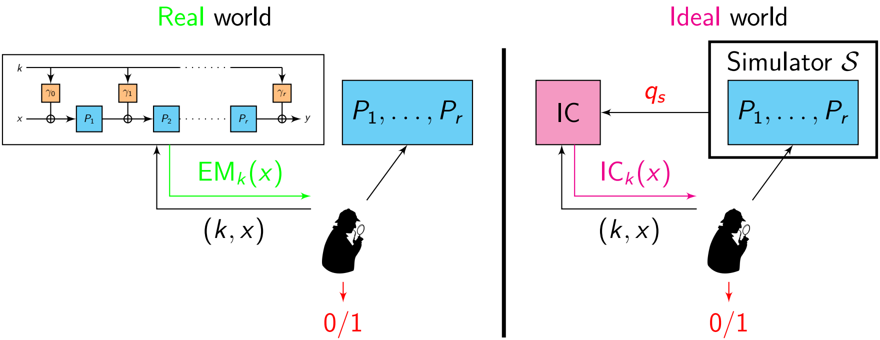
A block cipher construction is said (q_d, q_s, ε)-indifferentiable from an ideal cipher if there exists a simulator $\mathcal{S}$ such that for any distinguisher $\mathcal{D}$ making at most q_d queries in total, $\mathcal{S}$ makes at most q_s ideal cipher queries and $\mathcal{D}$ distinguishes the two worlds with adv. at most ε

Two Flavors of Indifferentiability



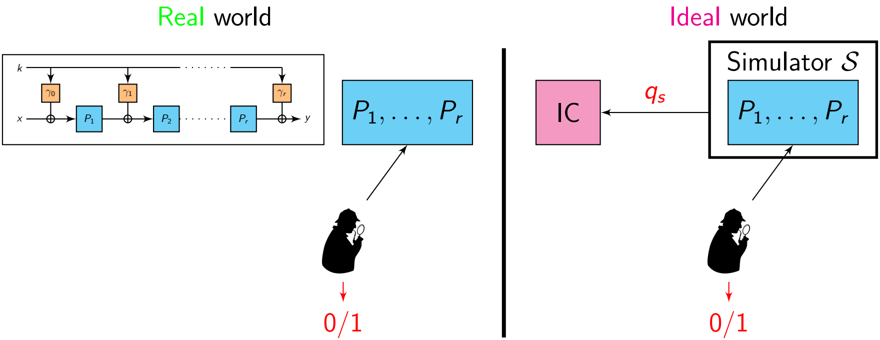
- full indifferentiability: $\mathcal{D}$ can queries its oracle as it wishes
- sequential indifferentiability: two query phases
  1. $\mathcal{D}$ first queries only P_i's/$\mathcal{S}$
  2. and then only EM/IC
- full indiff. $\Rightarrow$ sequential indiff.

Two Flavors of Indifferentiability



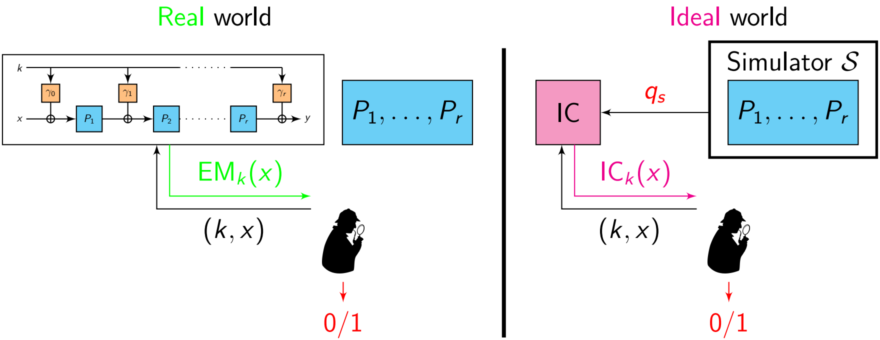
- full indifferentiability: $\mathcal{D}$ can queries its oracle as it wishes
- sequential indifferentiability: two query phases
    1. $\mathcal{D}$ first queries only P_i's/$\mathcal{S}$
    2. and then only EM/IC
- full indiff. $\Rightarrow$ sequential indiff.

Two Flavors of Indifferentiability



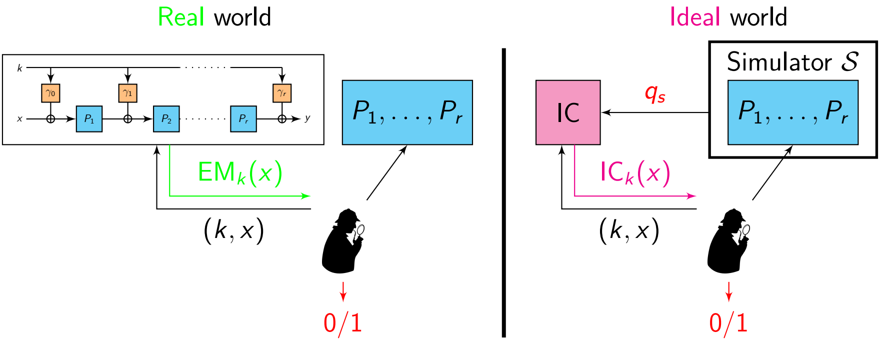
- full indifferentiability: $\mathcal{D}$ can queries its oracle as it wishes
- sequential indifferentiability: two query phases
  1. $\mathcal{D}$ first queries only P_i's/$\mathcal{S}$
  2. and then only EM/IC
- full indiff. $\Rightarrow$ sequential indiff.

Two Flavors of Indifferentiability



- full indifferentiability: $\mathcal{D}$ can queries its oracle as it wishes
- sequential indifferentiability: two query phases
  1. $\mathcal{D}$ first queries only P_i's/$\mathcal{S}$
  2. and then only EM/IC
- full indiff. $\Rightarrow$ sequential indiff.

Two Flavors of Indifferentiability



- full indifferentiability: $\mathcal{D}$ can queries its oracle as it wishes
- sequential indifferentiability: two query phases
  1. $\mathcal{D}$ first queries only P_i's/$\mathcal{S}$
  2. and then only EM/IC
- full indiff. $\Rightarrow$ sequential indiff.

Composition Theorems

Theorem (Composition for full indiff. [MRH04])

Informally, if a block cipher construction $\mathcal{C}^F$ is full-indifferentiable from an ideal cipher, then any cryptosystem proven secure with an ideal cipher remains provably secure when used with $\mathcal{C}^F$ (for cryptosystems whose security is defined by a single-stage game [RSS11]).

Theorem ([MPS12, CS15])

If a block cipher construction $\mathcal{C}^F$ is (q_d, q_s, ε)-seq-indiff. from an ideal cipher, and if a relation $\mathcal{R}$ is $(q_s, \varepsilon_{\mathrm{ic}})$-evasive for an ideal cipher, then $\mathcal{C}^F$ is $(q_d, \varepsilon_{\mathrm{ic}} + \varepsilon)$-correlation intractable w.r.t. $\mathcal{R}$.

	IC		$\mathcal{C}^F$
queries	q_s	$\xrightarrow{(q_d, q_s, \varepsilon)\text{-seq-indiff.}}$	q_d
success proba.	$\varepsilon_{\mathrm{ic}}$		$\varepsilon_{\mathrm{ic}} + \varepsilon$

Composition Theorems

Theorem (Composition for full indiff. [MRH04])

Informally, if a block cipher construction $\mathcal{C}^F$ is full-indifferentiable from an ideal cipher, then any cryptosystem proven secure with an ideal cipher remains provably secure when used with $\mathcal{C}^F$ (for cryptosystems whose security is defined by a single-stage game [RSS11]).

Theorem ([MPS12, CS15])

If a block cipher construction $\mathcal{C}^F$ is (q_d, q_s, ε)-seq-indiff. from an ideal cipher, and if a relation $\mathcal{R}$ is $(q_s, \varepsilon_{\mathrm{ic}})$-evasive for an ideal cipher, then $\mathcal{C}^F$ is $(q_d, \varepsilon_{\mathrm{ic}} + \varepsilon)$-correlation intractable w.r.t. $\mathcal{R}$.

	IC		$\mathcal{C}^F$
queries	q_s	(q_d, q_s, ε)-seq-indiff. $\longrightarrow$	q_d
success proba.	$\varepsilon_{\mathrm{ic}}$		$\varepsilon_{\mathrm{ic}} + \varepsilon$

Composition Theorems

Theorem (Composition for full indiff. [MRH04])

Informally, if a block cipher construction $\mathcal{C}^F$ is full-indifferentiable from an ideal cipher, then any cryptosystem proven secure with an ideal cipher remains provably secure when used with $\mathcal{C}^F$ (for cryptosystems whose security is defined by a single-stage game [RSS11]).

Theorem ([MPS12, CS15])

If a block cipher construction $\mathcal{C}^F$ is (q_d, q_s, ε)-seq-indiff. from an ideal cipher, and if a relation $\mathcal{R}$ is $(q_s, \varepsilon_{\mathrm{ic}})$-evasive for an ideal cipher, then $\mathcal{C}^F$ is $(q_d, \varepsilon_{\mathrm{ic}} + \varepsilon)$-correlation intractable w.r.t. $\mathcal{R}$.

	IC		$\mathcal{C}^F$
queries	q_s	$\xrightarrow{(q_d, q_s, \varepsilon)\text{-seq-indiff.}}$	q_d
success proba.	$\varepsilon_{\mathrm{ic}}$		$\varepsilon_{\mathrm{ic}} + \varepsilon$

Indifferentiability Results for the IEM Cipher

Theorem (Andreeva *et al.* [ABD+13])

The 5-round IEM cipher with a key-schedule modeled as a random oracle is fully indifferentiable from an ideal cipher.

NB: strong assumption on the key-schedule (often invertible in real BCs)

Theorem (Lampe-Seurin [LS13])

The 12-round IEM cipher with the trivial key-schedule is fully indifferentiable from an ideal cipher.

Theorem (Cogliati-Seurin [CS15])

The 4-round IEM cipher with the trivial key-schedule is sequentially indifferentiable from an ideal cipher with $q_s = \mathcal{O}(q_d^2)$ and $\varepsilon = \mathcal{O}(q_d^4/2^n)$

Indifferentiability Results for the IEM Cipher

Theorem (Andreeva *et al.* [ABD+13])

The 5-round IEM cipher with a key-schedule modeled as a random oracle is fully indifferentiable from an ideal cipher.

NB: strong assumption on the key-schedule (often invertible in real BCs)

Theorem (Lampe-Seurin [LS13])

The 12-round IEM cipher with the trivial key-schedule is fully indifferentiable from an ideal cipher.

Theorem (Cogliati-Seurin [CS15])

The 4-round IEM cipher with the trivial key-schedule is sequentially indifferentiable from an ideal cipher with $q_s = \mathcal{O}(q_d^2)$ and $\varepsilon = \mathcal{O}(q_d^4/2^n)$

Indifferentiability Results for the IEM Cipher

Theorem (Andreeva *et al.* [ABD+13])

The 5-round IEM cipher with a key-schedule modeled as a random oracle is fully indifferentiable from an ideal cipher.

NB: strong assumption on the key-schedule (often invertible in real BCs)

Theorem (Lampe-Seurin [LS13])

The 12-round IEM cipher with the trivial key-schedule is fully indifferentiable from an ideal cipher.

Theorem (Cogliati-Seurin [CS15])

The 4-round IEM cipher with the trivial key-schedule is sequentially indifferentiable from an ideal cipher with $q_s = \mathcal{O}(q_d^2)$ *and* $\varepsilon = \mathcal{O}(q_d^4/2^n)$

CKA Resistance for the 4-Round IEM Cipher

By the composition theorem "seq-indiff. $\Rightarrow$ correlation-intractability":

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

By the composition theorem "seq-indiff. $\Rightarrow$ correlation-intractability":

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

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:

- pseudorandomness for non-independent round keys, $r \geq 3$
- full indifferentiability:
  - best known attack is only on 3 rounds (for trivial KS)
  - minimal number of rounds for full indifferentiability ? ($4 \leq r \leq 12$)
  - $\Rightarrow$ the 4-round IEM might already be fully indifferentiable from an IC

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:

- pseudorandomness for non-independent round keys, $r \geq 3$
- full indifferentiability:
  - best known attack is only on 3 rounds (for trivial KS)
  - minimal number of rounds for full indifferentiability ? ($4 \leq r \leq 12$)
  - $\Rightarrow$ the 4-round IEM might already be fully indifferentiable from an IC

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:

- pseudorandomness for non-independent round keys, $r \geq 3$
- full indifferentiability:
  - best known attack is only on 3 rounds (for trivial KS)
  - minimal number of rounds for full indifferentiability ? ($4 \leq r \leq 12$)
  - $\Rightarrow$ the 4-round IEM might already be fully indifferentiable from an IC

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:

- pseudorandomness for non-independent round keys, $r \geq 3$
- full indifferentiability:
  - best known attack is only on 3 rounds (for trivial KS)
  - minimal number of rounds for full indifferentiability ? ($4 \leq r \leq 12$)
  - $\Rightarrow$ the 4-round IEM might already be fully indifferentiable from an IC

Summary of Known Results

Security notion	# of rounds	Key schedule	Security bound	Simul. (q_S/t_S)	Ref.
Single-key	$r \geq 1$	independent	$2^{\frac{rn}{r+1}}$	—	[CS14]
	1	trivial	$2^{\frac{n}{2}}$	—	[EM97, DKS12]
	2	trivial	$2^{\frac{2n}{3}}$	—	[CLL+14]
XOR RKA	3	trivial	$2^{\frac{n}{2}}$	—	[CS15, FP15]
	1	nonlinear	$2^{\frac{n}{2}}$	—	[CS15]
CKA (Seq-ind.)	4	trivial	$2^{\frac{n}{4}}$	q^2 / q^2	[CS15]
Full indiff.	5	rand. oracle	$2^{\frac{n}{10}}$	q^2 / q^3	[ABD+13]
	12	trivial	$2^{\frac{n}{12}}$	q^4 / q^6	[LS13]

The End...

Thanks for your attention!

Comments or questions?

References I

Elena Andreeva, Andrey Bogdanov, Yevgeniy Dodis, Bart Mennink, and John P. Steinberger. On the Indifferentiability of Key-Alternating Ciphers. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 (Proceedings, Part I)*, volume 8042 of *LNCS*, pages 531–550. Springer, 2013. Full version available at `http://eprint.iacr.org/2013/061`.

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.

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 *LNCS*, pages 45–62. Springer, 2012.

References II

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.

Shan Chen, Rodolphe Lampe, Jooyoung Lee, Yannick Seurin, and John P. Steinberger. Minimizing the Two-Round Even-Mansour Cipher. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 (Proceedings, Part I)*, volume 8616 of *LNCS*, pages 39–56. Springer, 2014. Full version available at `http://eprint.iacr.org/2014/443`.

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`.

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`.

References III

Joan Daemen. Limitations of the Even-Mansour Construction. In Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors, *Advances in Cryptology - ASIACRYPT '91*, volume 739 of *LNCS*, pages 495–498. Springer, 1991.

Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Key Recovery Attacks on 3-round Even-Mansour, 8-step LED-128, and Full AES^2. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 (Proceedings, Part I)*, volume 8269 of *LNCS*, pages 337–356. Springer, 2013. Full version available at `http://eprint.iacr.org/2013/391`.

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.

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

References IV

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.

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 *LNCS*, pages 278–295. Springer, 2012.

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.

Avradip Mandal, Jacques Patarin, and Yannick Seurin. On the Public Indifferentiability and Correlation Intractability of the 6-Round Feistel Construction. In Ronald Cramer, editor, *Theory of Cryptography Conference - TCC 2012*, volume 7194 of *LNCS*, pages 285–302. Springer, 2012. Full version available at http://eprint.iacr.org/2011/496.

References V

Ueli M. Maurer, Renato Renner, and Clemens Holenstein. Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology. In Moni Naor, editor, *Theory of Cryptography Conference- TCC 2004*, volume 2951 of *LNCS*, pages 21–39. Springer, 2004.

Thomas Ristenpart, Hovav Shacham, and Thomas Shrimpton. Careful with Composition: Limitations of the Indifferentiability Framework. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 487–506. Springer, 2011.

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`.