Relaxing Full-Codebook Security: A Refined Analysis of Key-Length Extension Schemes

Peter Gaži[1] Jooyoung Lee[2]
Yannick Seurin[3] John Steinberger[4] Stefano Tessaro[5]

[1]IST, Austria

[2]Sejong University, Korea

[3]ANSSI, France

[4]Tsinghua University, China

[5]UC Santa Barbara, USA

March 10, 2015 - FSE 2015

Outline

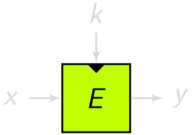
Context: Key-Length Extension for Block Ciphers

Main Lemma

Randomized Cascading

Plain Cascading

Block Ciphers



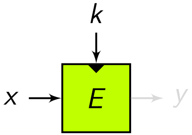
A block cipher E

- takes as input
  - a plaintext $x \in \{0,1\}^n$
  - a key $k \in \{0,1\}^\kappa$
- outputs a ciphertext $y \in \{0,1\}^n$
- $E_k(\cdot)$ is a permutation $\forall k$
- examples: DES, AES, IDEA, etc.

Notation

- n = block-length
- κ = key-length

Block Ciphers



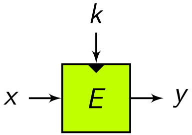
A block cipher E

- takes as input
  - a plaintext $x \in \{0,1\}^n$
  - a key $k \in \{0,1\}^\kappa$
- outputs a ciphertext $y \in \{0,1\}^n$
- $E_k(\cdot)$ is a permutation $\forall k$
- examples: DES, AES, IDEA, etc.

Notation

- n = block-length
- κ = key-length

Block Ciphers



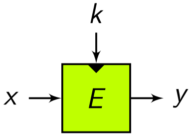
A block cipher E

- takes as input
  - a plaintext $x \in \{0,1\}^n$
  - a key $k \in \{0,1\}^\kappa$
- outputs a ciphertext $y \in \{0,1\}^n$
- $E_k(\cdot)$ is a permutation $\forall k$
- examples: DES, AES, IDEA, etc.

Notation

- n = block-length
- κ = key-length

Block Ciphers



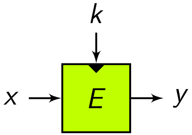
A block cipher E

- takes as input
  - a plaintext $x \in \{0,1\}^n$
  - a key $k \in \{0,1\}^\kappa$
- outputs a ciphertext $y \in \{0,1\}^n$
- $E_k(\cdot)$ is a permutation $\forall k$
- examples: DES, AES, IDEA, etc.

Notation

- n = block-length
- κ = key-length

Block Ciphers



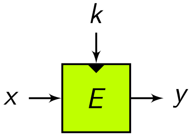
A block cipher E

- takes as input
  - a plaintext $x \in \{0,1\}^n$
  - a key $k \in \{0,1\}^\kappa$
- outputs a ciphertext $y \in \{0,1\}^n$
- $E_k(\cdot)$ is a permutation $\forall k$
- examples: DES, AES, IDEA, etc.

Notation

- n = block-length
- κ = key-length

Block Ciphers



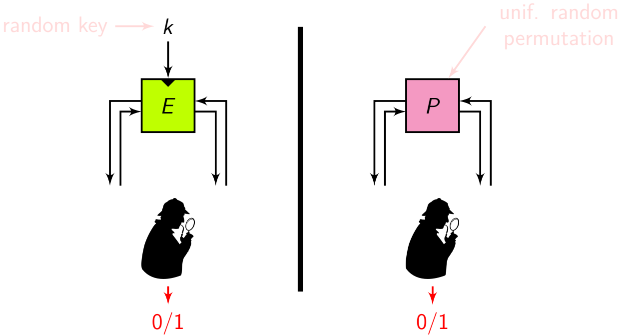
A block cipher E

- takes as input
  - a plaintext $x \in \{0,1\}^n$
  - a key $k \in \{0,1\}^\kappa$
- outputs a ciphertext $y \in \{0,1\}^n$
- $E_k(\cdot)$ is a permutation $\forall k$
- examples: DES, AES, IDEA, etc.

Notation

- n = block-length
- κ = key-length

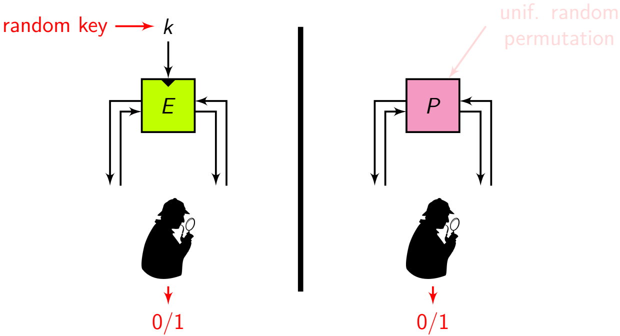
Block Cipher Security: Pseudorandom Permutations



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

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

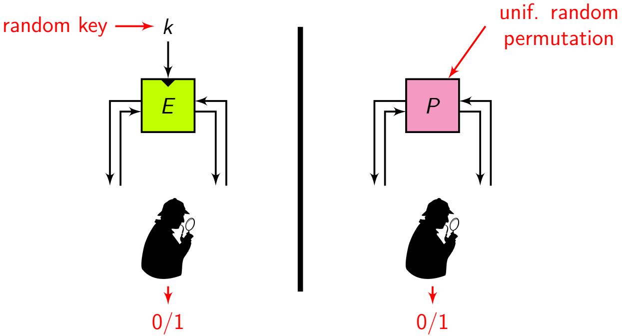
Block Cipher Security: Pseudorandom Permutations



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

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

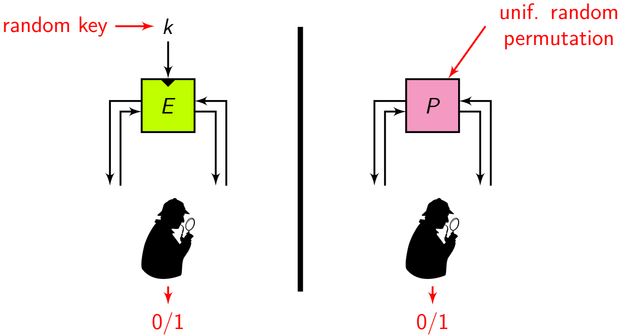
Block Cipher Security: Pseudorandom Permutations



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

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

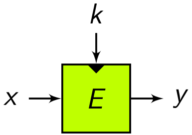
Block Cipher Security: Pseudorandom Permutations



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

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

Key-Length is Crucial



Exhaustive key search

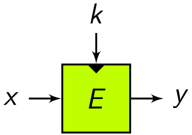
- key k is recoverable in $\sim 2^{\kappa}$ evaluations of E

Given $\mathcal{O} \in \{P, E_k\}$:

1. $y \leftarrow \mathcal{O}(0^n)$
2. $\forall k' \in \{0,1\}^{\kappa}$:
   (a) $y' \leftarrow E_{k'}(0^n)$
   (b) if $y = y'$, check k' with some extra queries

- this also upper bounds PRP-security!
- this is a generic attack (works for any E)

Key-Length is Crucial

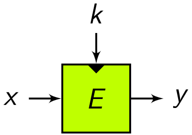


Exhaustive key search

- key k is recoverable in $\sim 2^{\kappa}$ evaluations of E

  Given $\mathcal{O} \in \{P, E_k\}$:
  1. $y \leftarrow \mathcal{O}(0^n)$
  2. $\forall k' \in \{0,1\}^{\kappa}$:
     (a) $y' \leftarrow E_{k'}(0^n)$
     (b) if $y = y'$, check k' with some extra queries
- this also upper bounds PRP-security!
- this is a generic attack (works for any E)

Key-Length is Crucial



Exhaustive key search

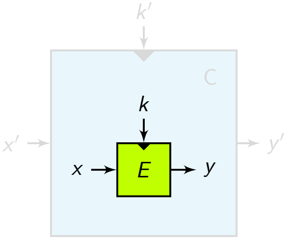
- key k is recoverable in $\sim 2^{\kappa}$ evaluations of E

  Given $\mathcal{O} \in \{P, E_k\}$:

  1. $y \leftarrow \mathcal{O}(0^n)$
  2. $\forall k' \in \{0,1\}^{\kappa}$:
     (a) $y' \leftarrow E_{k'}(0^n)$
     (b) if $y = y'$, check k' with some extra queries

- this also upper bounds PRP-security!
- this is a generic attack (works for any E)

The Key-Length Extension (KLE) Problem



Goal:

construct from E a new block cipher

$$\mathrm{C}[E] : \{0,1\}^{\kappa'} \times \{0,1\}^n \to \{0,1\}^n$$

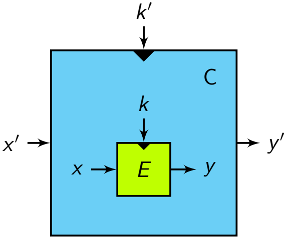
such that

- $\kappa' > \kappa$
- best generic attack requires $> 2^{\kappa}$ evaluations of E and C

Examples

- Triple Encryption
- FX construction (generic DESX)

The Key-Length Extension (KLE) Problem



Goal:

construct from E a new block cipher

$$\mathsf{C}[E] : \{0,1\}^{\kappa'} \times \{0,1\}^n \to \{0,1\}^n$$

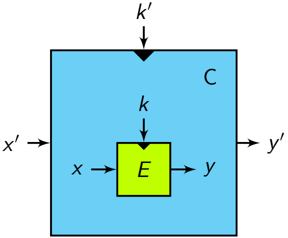
such that

- $\kappa' > \kappa$
- best generic attack requires $> 2^{\kappa}$ evaluations of E and C

Examples

- Triple Encryption
- FX construction (generic DESX)

The Key-Length Extension (KLE) Problem



Goal:
construct from E a new block cipher

$$\mathrm{C}[E] : \{0,1\}^{\kappa'} \times \{0,1\}^n \to \{0,1\}^n$$

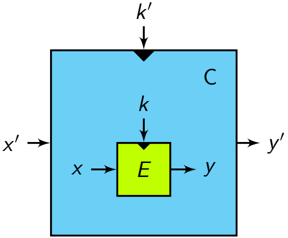
such that

- $\kappa' > \kappa$
- best generic attack requires $> 2^{\kappa}$ evaluations of E and C

Examples

- Triple Encryption
- FX construction (generic DESX)

The Key-Length Extension (KLE) Problem



Goal:

construct from E a new block cipher

$$\mathrm{C}[E] : \{0,1\}^{\kappa'} \times \{0,1\}^n \rightarrow \{0,1\}^n$$

such that

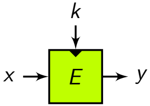
- $\kappa' > \kappa$
- best generic attack requires $> 2^{\kappa}$ evaluations of E and C

Examples

- Triple Encryption
- FX construction (generic DESX)

The Ideal Cipher Model (ICM)

We will model the underlying block cipher E as an ideal cipher



Ideal Block Cipher Model

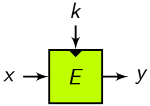
- family of uniformly random permutations $E_k(\cdot)$
- independent for each key
- given as an oracle to all parties (incl. adversaries)

Generic Security

- attacks cannot exploit any weakness of E
  $\Rightarrow$ “generic” attacks

The Ideal Cipher Model (ICM)

We will model the underlying block cipher E as an ideal cipher



Ideal Block Cipher Model

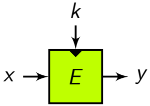
- family of uniformly random permutations $E_k(\cdot)$
- independent for each key
- given as an oracle to all parties (incl. adversaries)

Generic Security

- attacks cannot exploit any weakness of E
  $\Rightarrow$ "generic" attacks

The Ideal Cipher Model (ICM)

We will model the underlying block cipher E as an ideal cipher



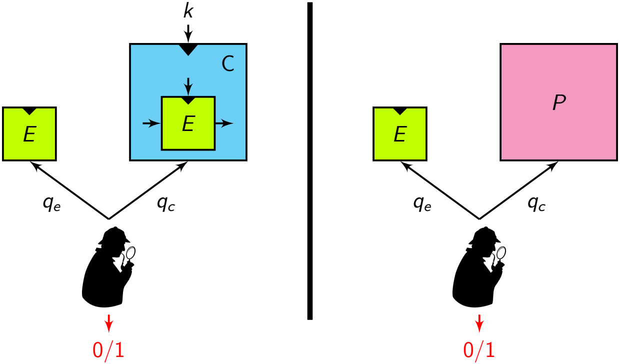
Ideal Block Cipher Model

- family of uniformly random permutations $E_k(\cdot)$
- independent for each key
- given as an oracle to all parties (incl. adversaries)

Generic Security

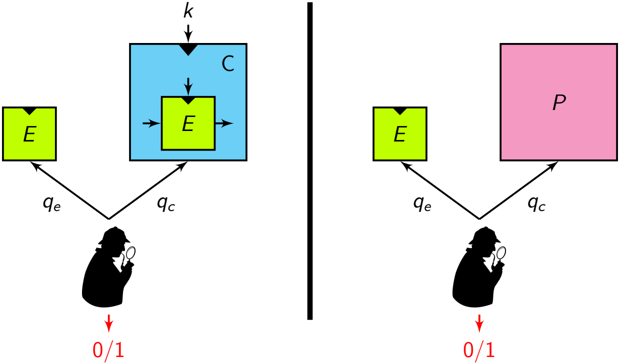
- attacks cannot exploit any weakness of E
  $\Rightarrow$ "generic" attacks

Key-Length Extension in the ICM



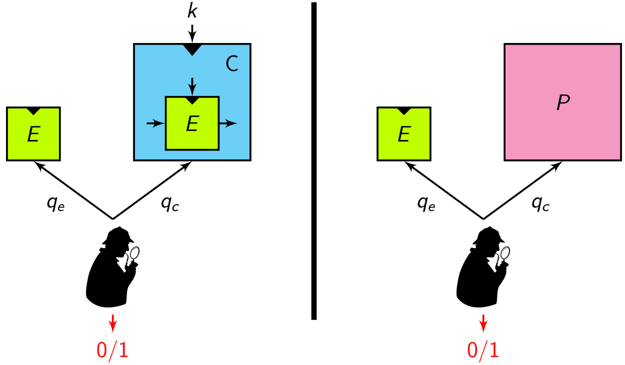
- q_c construction queries to $\mathsf{C}_k[E](\cdot)$ or $P(\cdot)$
- q_e ideal cipher queries to $E(\cdot,\cdot)$
- it is computationally unbounded (information-theoretic sec.)
- NB: generic attack with $q_e = 2^{\kappa+n}$ for any KLE scheme

Key-Length Extension in the ICM



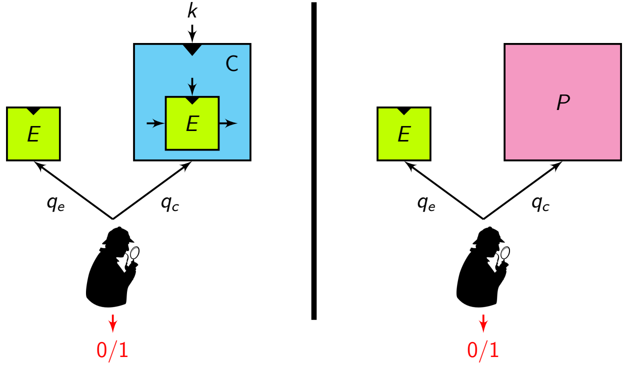
- q_c construction queries to $C_k[E](\cdot)$ or $P(\cdot)$
- q_e ideal cipher queries to $E(\cdot,\cdot)$
- it is computationally unbounded (information-theoretic sec.)
- NB: generic attack with $q_e = 2^{\kappa+n}$ for any KLE scheme

Key-Length Extension in the ICM



- q_c construction queries to $C_k[E](\cdot)$ or $P(\cdot)$
- q_e ideal cipher queries to $E(\cdot,\cdot)$
- it is computationally unbounded (information-theoretic sec.)
- NB: generic attack with $q_e = 2^{\kappa+n}$ for any KLE scheme

Key-Length Extension in the ICM

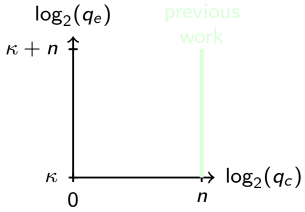


- q_c construction queries to $\mathsf{C}_k[E](\cdot)$ or $P(\cdot)$
- q_e ideal cipher queries to $E(\cdot,\cdot)$
- it is computationally unbounded (information-theoretic sec.)
- NB: generic attack with $q_e = 2^{\kappa+n}$ for any KLE scheme

Full vs. Partial Codebook

Query Accounting

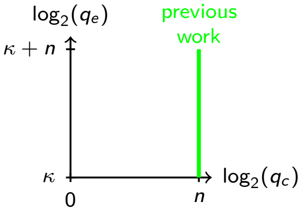
- most previous work sets $q_c = 2^n$ (*full codebook* of C[E])
  $\Rightarrow q_e$ is the only complexity measure
- too restrictive!
  - number of pt/ct pairs can be limited (frequent rekeying)
  - mode of operation may impose $q_c \ll 2^n$
- we aim at studying the entire plan (q_c, q_e)



Full vs. Partial Codebook

Query Accounting

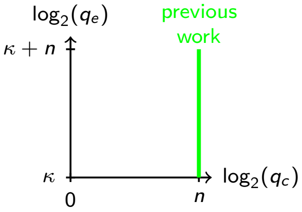
- most previous work sets $q_c = 2^n$ (*full codebook* of C[E])
  $\Rightarrow q_e$ is the only complexity measure
- too restrictive!
  - number of pt/ct pairs can be limited (frequent rekeying)
  - mode of operation may impose $q_c \ll 2^n$
- we aim at studying the entire plan (q_c, q_e)



Full vs. Partial Codebook

Query Accounting

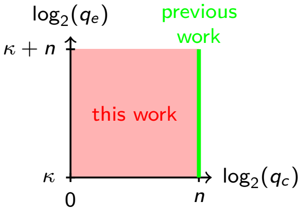
- most previous work sets $q_c = 2^n$ (*full codebook* of C[E])
  $\Rightarrow q_e$ is the only complexity measure
- too restrictive!
  - number of pt/ct pairs can be limited (frequent rekeying)
  - mode of operation may impose $q_c \ll 2^n$
- we aim at studying the entire plan (q_c, q_e)



Full vs. Partial Codebook

Query Accounting

- most previous work sets $q_c = 2^n$ (*full codebook* of $\mathsf{C}[E]$)
  $\Rightarrow q_e$ is the only complexity measure
- too restrictive!
  - number of pt/ct pairs can be limited (frequent rekeying)
  - mode of operation may impose $q_c \ll 2^n$
- we aim at studying the entire plan (q_c, q_e)



Outline

Context: Key-Length Extension for Block Ciphers

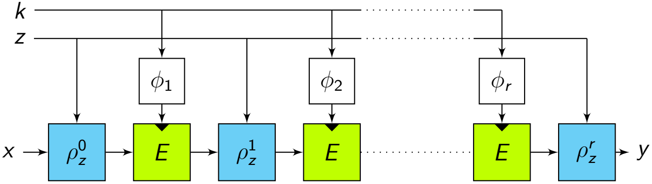
Main Lemma

Randomized Cascading

Plain Cascading

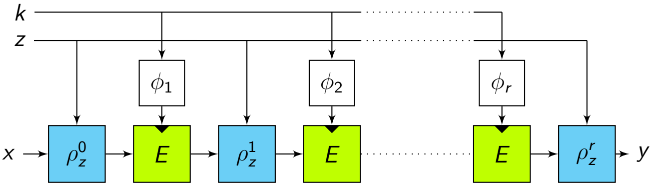
Randomized Key-Length Extension Schemes

Very general class abiding to the following structure:



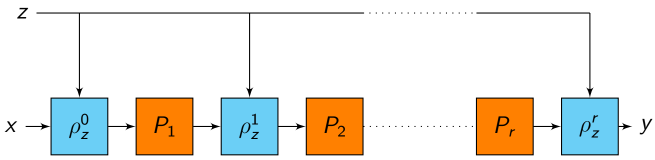
- the ρ^i's are keyed permutations, potentially very simple (e.g. $\rho_z^i(x) = x \oplus z$)
- encryption keys $\phi_1(k), \ldots, \phi_r(k)$ can be deterministically related or independent

Induced Sequential Cipher



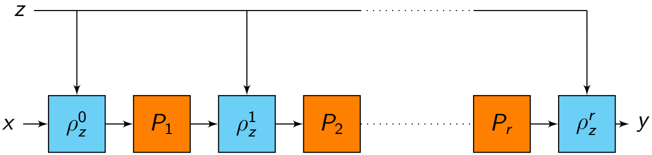
- k fixed and known
  $\Rightarrow$ C[E] = block cipher construction using
  - independent public permutations $P_1, \ldots, P_r$
  - key z
- $\Rightarrow$ induced sequential cipher (ISC) of C, denoted $\overline{\mathrm{C}}$
- generalization of a key-alternating cipher
- well-studied design in the Random Permutation Model

Induced Sequential Cipher



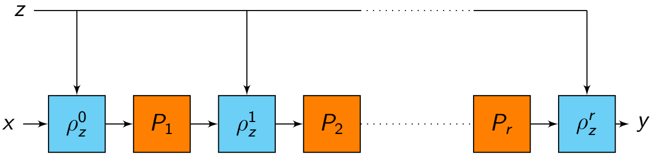
- k fixed and known
  $\Rightarrow$ C$[E]$ = block cipher construction using
  - independent public permutations $P_1, \ldots, P_r$
  - key z
- $\Rightarrow$ induced sequential cipher (ISC) of C, denoted $\overline{\mathrm{C}}$
- generalization of a key-alternating cipher
- well-studied design in the Random Permutation Model

Induced Sequential Cipher



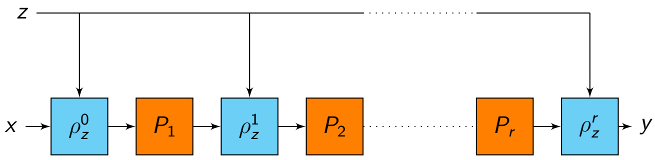
- k fixed and known
  $\Rightarrow$ C[E] = block cipher construction using
  - independent public permutations $P_1, \ldots, P_r$
  - key z
- $\Rightarrow$ induced sequential cipher (ISC) of C, denoted $\overline{\mathrm{C}}$
- generalization of a key-alternating cipher
- well-studied design in the Random Permutation Model

Induced Sequential Cipher



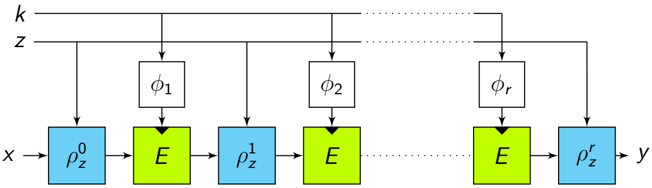
- k fixed and known
  $\Rightarrow$ C[E] = block cipher construction using
  - independent public permutations $P_1, \ldots, P_r$
  - key z
- $\Rightarrow$ induced sequential cipher (ISC) of C, denoted $\overline{\mathrm{C}}$
- generalization of a key-alternating cipher
- well-studied design in the Random Permutation Model

Induced Sequential Cipher



- k fixed and known
  $\Rightarrow$ C[E] = block cipher construction using
  - independent public permutations $P_1, \ldots, P_r$
  - key z
- $\Rightarrow$ induced sequential cipher (ISC) of C, denoted $\overline{\mathrm{C}}$
- generalization of a key-alternating cipher
- well-studied design in the Random Permutation Model

KLE-to-ISC Lemma



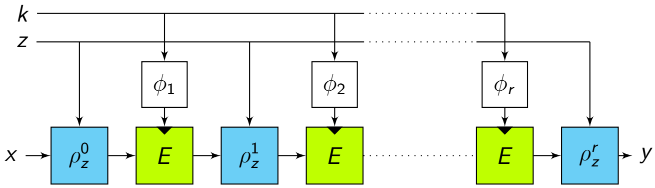
Allows to reduce the security analysis of a randomized KLE C to the analysis of the Induced Sequential Cipher $\overline{\mathsf{C}}$

Lemma

For any M,

Optimizing M yields a bound that depends only on q_c and q_e.

KLE-to-ISC Lemma



Allows to reduce the security analysis of a randomized KLE C to the analysis of the Induced Sequential Cipher $\overline{\mathrm{C}}$

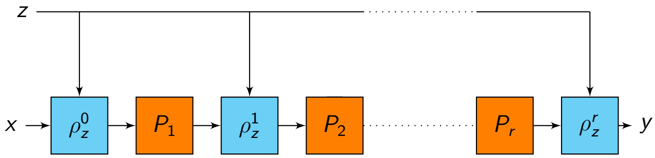
Lemma

For any M,

$$\mathbf{Adv}_{\mathrm{C}}^{\mathrm{sprp}}(q_c, q_e) \leq$$

Optimizing M yields a bound that depends only on q_c and q_e.

KLE-to-ISC Lemma



Allows to reduce the security analysis of a randomized KLE C to the analysis of the Induced Sequential Cipher $\overline{\mathsf{C}}$

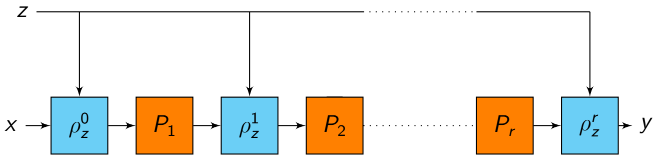
Lemma

For any M,

$$\mathbf{Adv}^{\mathrm{sprp}}_{\mathsf{C}}(q_c, q_e) \leq \frac{r q_e}{M 2^{\kappa}} + \mathbf{Adv}^{\mathrm{sprp}}_{\overline{\mathsf{C}}}(q_c, M)$$

Optimizing M yields a bound that depends only on q_c and q_e.

KLE-to-ISC Lemma



Allows to reduce the security analysis of a randomized KLE C to the analysis of the Induced Sequential Cipher $\overline{\mathsf{C}}$

Lemma

For any M,

$$\mathbf{Adv}_{\mathsf{C}}^{\mathrm{sprp}}(q_c, q_e) \leq \frac{rq_e}{M2^{\kappa}} + \mathbf{Adv}_{\overline{\mathsf{C}}}^{\mathrm{sprp}}(q_c, M)$$

Optimizing M yields a bound that depends only on q_c and q_e.

Outline

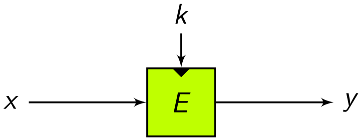
Context: Key-Length Extension for Block Ciphers

Main Lemma

Randomized Cascading

Plain Cascading

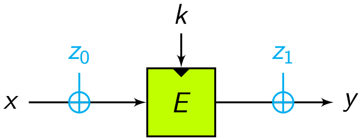
Key Whitening



FX construction (generic DESX)

- additional keys hide i./o. of E
- suggested by Rivest
- analyzed by [KR01]
- secure when $q_c \cdot q_e \ll 2^{\kappa+n}$
- same bound when $z_0 = z_1$

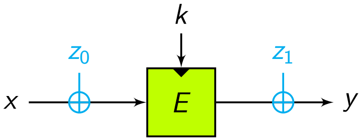
Key Whitening



FX construction (generic DESX)

- additional keys hide i./o. of E
- suggested by Rivest
- analyzed by [KR01]
- secure when $q_c \cdot q_e \ll 2^{\kappa+n}$
- same bound when $z_0 = z_1$

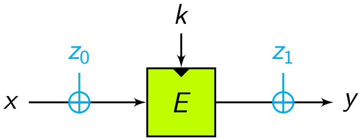
Key Whitening



FX construction (generic DESX)

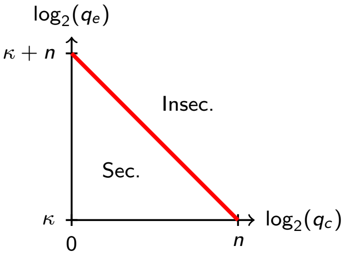
- additional keys hide i./o. of E
- suggested by Rivest
- analyzed by [KR01]
- secure when $q_c \cdot q_e \ll 2^{\kappa+n}$
- same bound when $z_0 = z_1$

Key Whitening

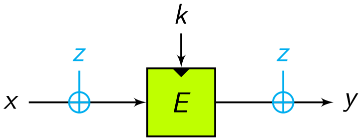


FX construction (generic DESX)

- additional keys hide i./o. of E
- suggested by Rivest
- analyzed by [KR01]
- secure when $q_c \cdot q_e \ll 2^{\kappa+n}$
- same bound when $z_0 = z_1$

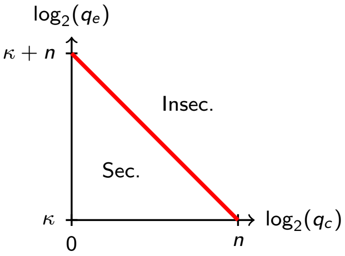


Key Whitening

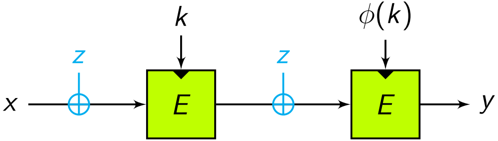


FX construction (generic DESX)

- additional keys hide i./o. of E
- suggested by Rivest
- analyzed by [KR01]
- secure when $q_c \cdot q_e \ll 2^{\kappa+n}$
- same bound when $z_0 = z_1$



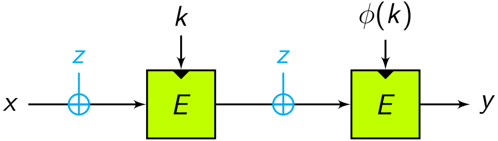
2XOR construction [GT12]



2XOR construction

- combines key-whitening and cascading
- same whitening key z
- ϕ such that $\forall k, \phi(k) \neq k$
- [GT12] proved (tight) security for $q_c = 2^n$ and $q_e \ll 2^{\kappa+n/2}$

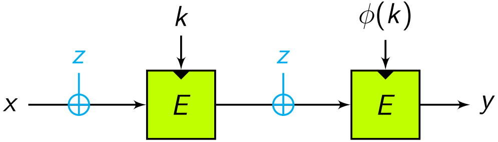
2XOR construction [GT12]



2XOR construction

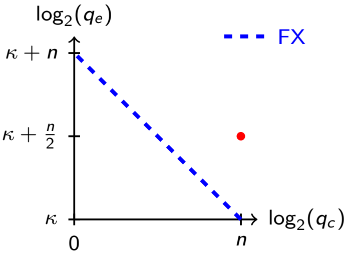
- combines key-whitening and cascading
- same whitening key z
- ϕ such that $\forall k,\ \phi(k) \neq k$
- [GT12] proved (tight) security for $q_c = 2^n$ and $q_e \ll 2^{\kappa+n/2}$

2XOR construction [GT12]

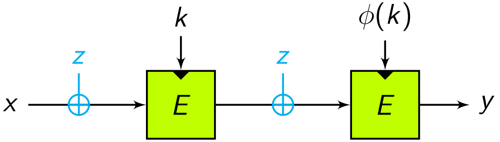


2XOR construction

- combines key-whitening and cascading
- same whitening key z
- ϕ such that $\forall k$, $\phi(k) \neq k$
- [GT12] proved (tight) security for $q_c = 2^n$ and $q_e \ll 2^{\kappa + n/2}$

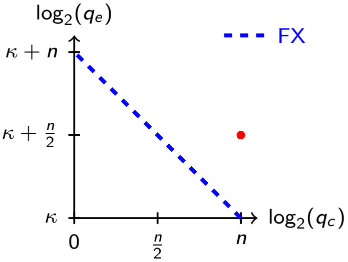


Refined Analysis of 2XOR

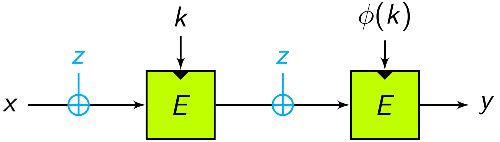


We (tightly) complete the picture:

- for $1 \leq q_c \leq 2^{n/2}$:
  same security bound as FX
- for $2^{n/2} \leq q_c \leq 2^n$:
  secure when $q_e \ll 2^{\kappa+n/2}$

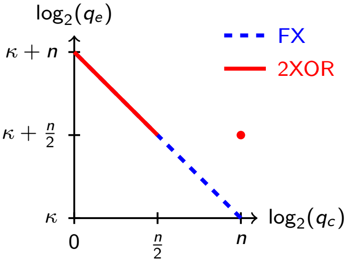


Refined Analysis of 2XOR

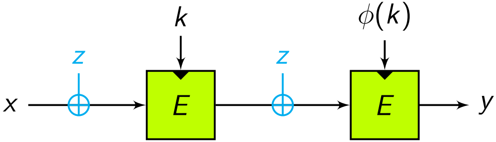


We (tightly) complete the picture:

- for $1 \le q_c \le 2^{n/2}$:
  same security bound as FX
- for $2^{n/2} \le q_c \le 2^n$:
  secure when $q_e \ll 2^{\kappa+n/2}$

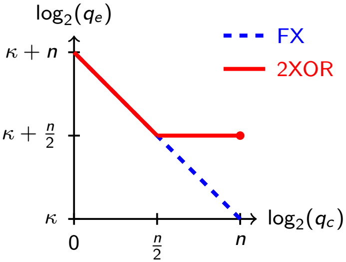


Refined Analysis of 2XOR

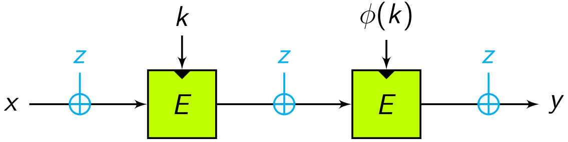


We (tightly) complete the picture:

- for $1 \leq q_c \leq 2^{n/2}$:
  same security bound as FX
- for $2^{n/2} \leq q_c \leq 2^n$:
  secure when $q_e \ll 2^{\kappa+n/2}$



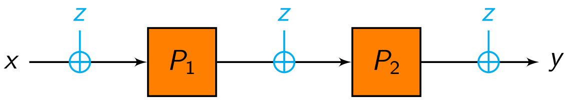
3XOR: Final Whitening Step Helps



3XOR construction

- add a final whitening step
- induced sequential cipher = 2-round Even-Mansour cipher with identical keys
  ⇒ analyzed by [CLL+14]
- we can apply the KLE-to-ISC Lemma

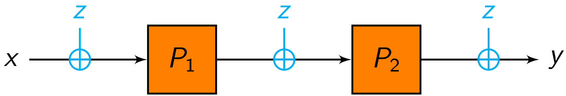
3XOR: Final Whitening Step Helps



3XOR construction

- add a final whitening step
- induced sequential cipher = 2-round Even-Mansour cipher with identical keys
  $\Rightarrow$ analyzed by [CLL$^+$14]
- we can apply the KLE-to-ISC Lemma

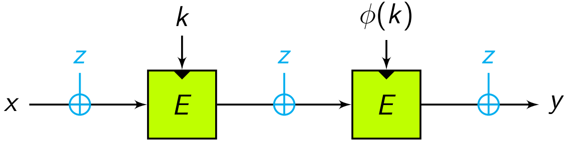
3XOR: Final Whitening Step Helps

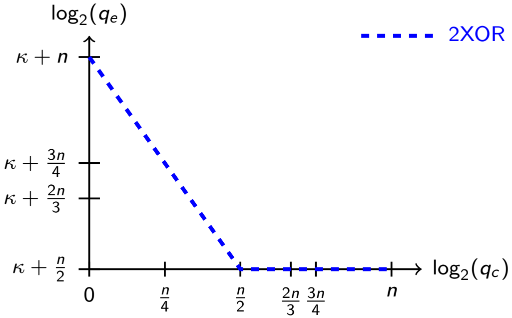


3XOR construction

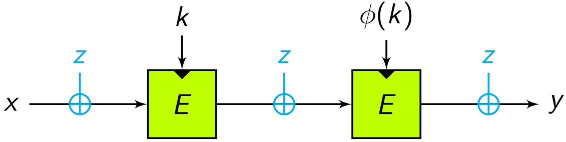
- add a final whitening step
- induced sequential cipher = 2-round Even-Mansour cipher with identical keys
  $\Rightarrow$ analyzed by [CLL$^+$14]
- we can apply the KLE-to-ISC Lemma

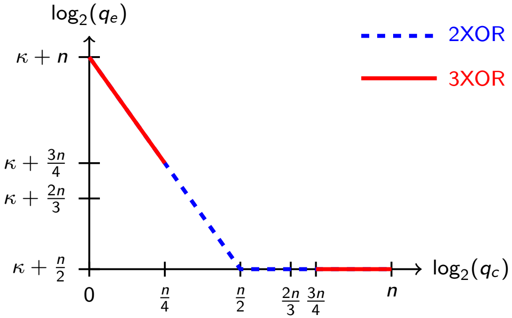
3XOR: Final Whitening Step Helps



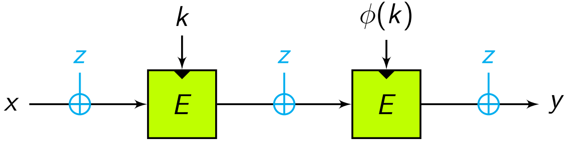


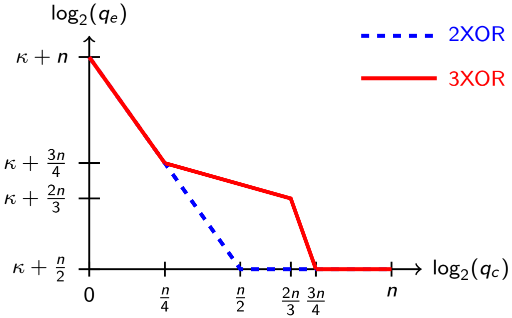
3XOR: Final Whitening Step Helps



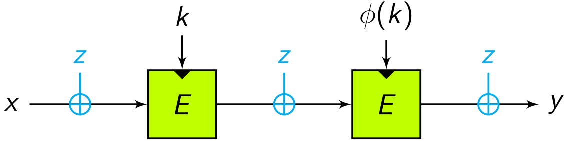


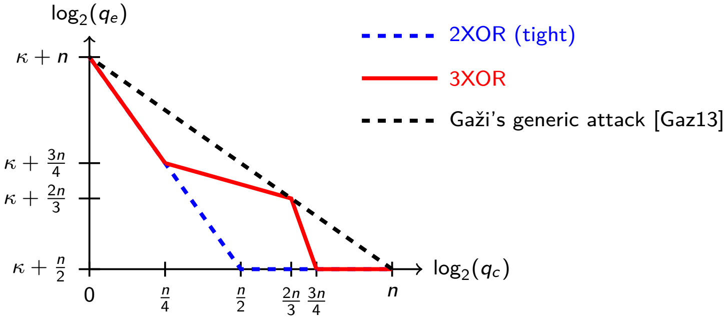
3XOR: Final Whitening Step Helps



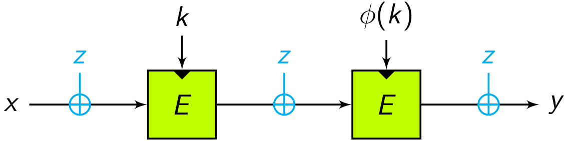


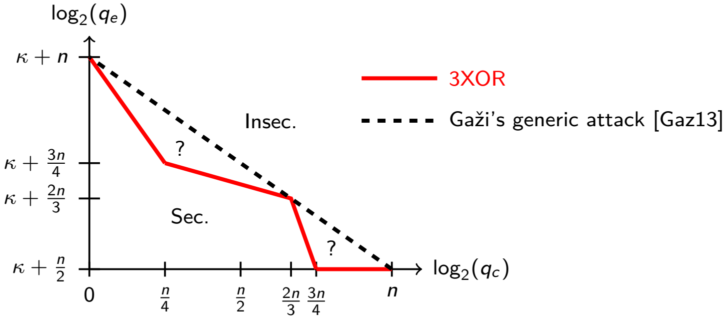
3XOR: Final Whitening Step Helps



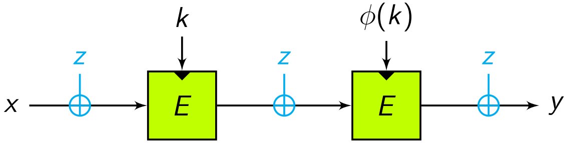


3XOR: Final Whitening Step Helps



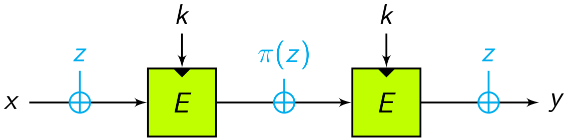


A 2-call Construction without Rekeying



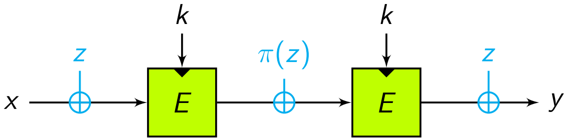
- drawback of 2XOR and 3XOR constructions: call the block cipher E with two distinct keys
- we propose a construction calling E twice with the same key
- π is a linear orthomorphism
- security bound qualitatively similar to 3XOR

A 2-call Construction without Rekeying



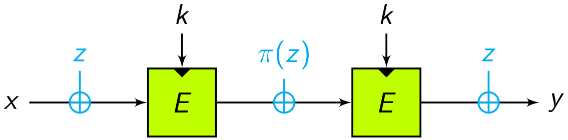
- drawback of 2XOR and 3XOR constructions: call the block cipher E with two distinct keys
- we propose a construction calling E twice with the same key
- π is a linear orthomorphism
- security bound qualitatively similar to 3XOR

A 2-call Construction without Rekeying



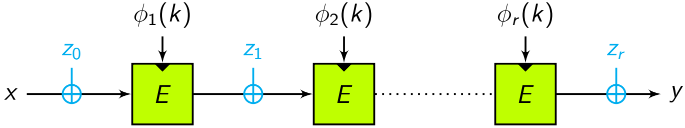
- drawback of 2XOR and 3XOR constructions:
  call the block cipher E with two distinct keys
- we propose a construction calling E twice with the same key
- π is a linear orthomorphism
- security bound qualitatively similar to 3XOR

A 2-call Construction without Rekeying



- drawback of 2XOR and 3XOR constructions: call the block cipher E with two distinct keys
- we propose a construction calling E twice with the same key
- π is a linear orthomorphism
- security bound qualitatively similar to 3XOR

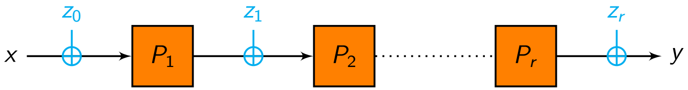
Independent Whitening Keys (XOR-Cascade)



Xor-Cascade Encryption: XCE

- independent whitening keys, distinct encryption keys
- induced sequential cipher = iterated Even-Mansour cipher $\Rightarrow$ tightly analyzed by Chen and Steinberger [CS14]
- r-round XCE is secure as long as $q_c \cdot q_e^r \ll 2^{r(\kappa+n)}$
- matched by Gaži's attack [Gaz13]

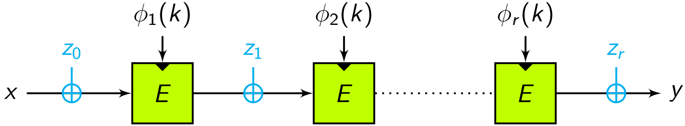
Independent Whitening Keys (XOR-Cascade)



Xor-Cascade Encryption: XCE

- independent whitening keys, distinct encryption keys
- induced sequential cipher = iterated Even-Mansour cipher
  $\Rightarrow$ tightly analyzed by Chen and Steinberger [CS14]
- r-round XCE is secure as long as $q_c \cdot q_e^r \ll 2^{r(\kappa+n)}$
- matched by Gaži's attack [Gaz13]

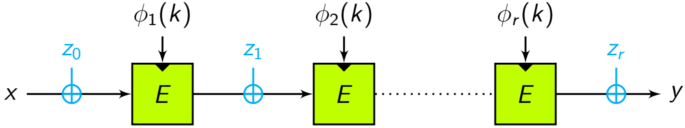
Independent Whitening Keys (XOR-Cascade)



Xor-Cascade Encryption: XCE

- independent whitening keys, distinct encryption keys
- induced sequential cipher = iterated Even-Mansour cipher
  $\Rightarrow$ tightly analyzed by Chen and Steinberger [CS14]
- r-round XCE is secure as long as $q_c \cdot q_e^r \ll 2^{r(\kappa+n)}$
- matched by Gaži's attack [Gaz13]

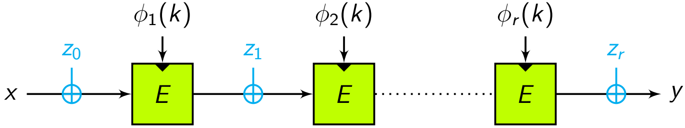
Independent Whitening Keys (XOR-Cascade)

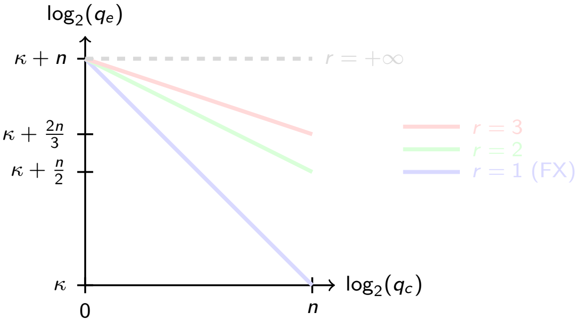


Xor-Cascade Encryption: XCE

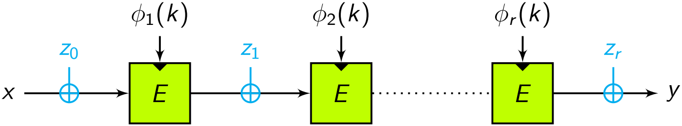
- independent whitening keys, distinct encryption keys
- induced sequential cipher = iterated Even-Mansour cipher
  $\Rightarrow$ tightly analyzed by Chen and Steinberger [CS14]
- r-round XCE is secure as long as $q_c \cdot q_e^r \ll 2^{r(\kappa+n)}$
- matched by Gaži's attack [Gaz13]

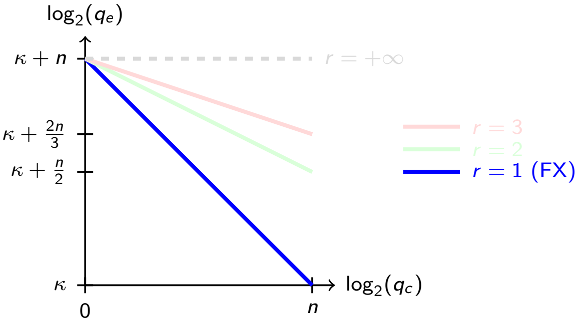
Independent Whitening Keys (XOR-Cascade)



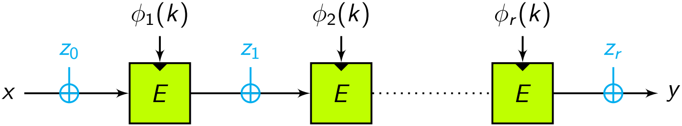


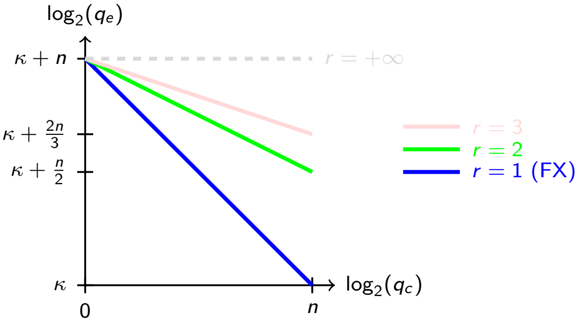
Independent Whitening Keys (XOR-Cascade)



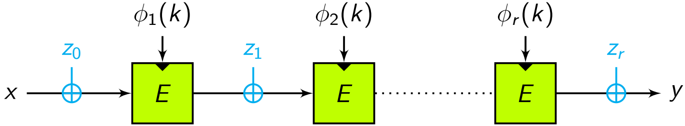


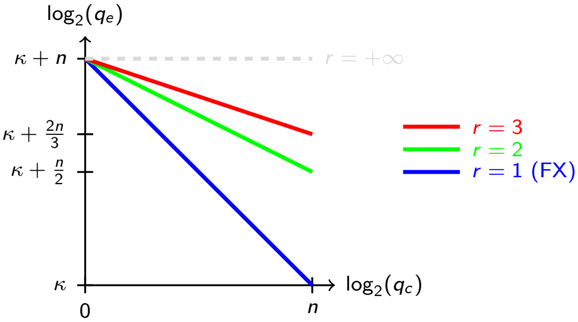
Independent Whitening Keys (XOR-Cascade)



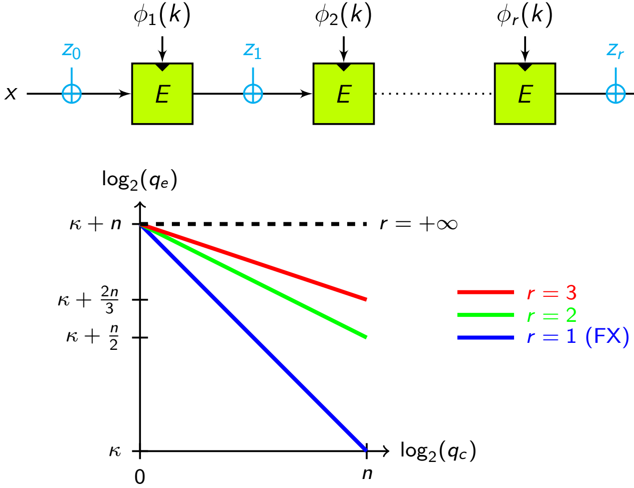


Independent Whitening Keys (XOR-Cascade)





Independent Whitening Keys (XOR-Cascade)



Outline

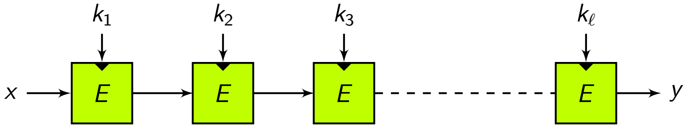
Context: Key-Length Extension for Block Ciphers

Main Lemma

Randomized Cascading

Plain Cascading

Plain Cascade Encryption

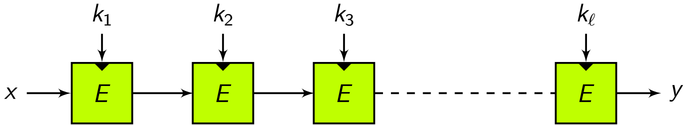


Cascade Encryption

- encrypt ℓ times with independent keys
- $\ell = 2$ does not help (meet-in-the-middle attack [DH77])
- security gain starting from $\ell = 3$ [BR06]
- tight bound for $q_c = 2^n$ [DLMS14]: for odd ℓ, secure when

$$q_e \ll 2^{\kappa + \frac{\ell-1}{\ell+1} n}$$

Plain Cascade Encryption

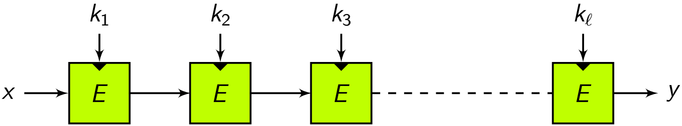


Cascade Encryption

- encrypt ℓ times with independent keys
- $\ell = 2$ does not help (meet-in-the-middle attack [DH77])
- security gain starting from $\ell = 3$ [BR06]
- tight bound for $q_c = 2^n$ [DLMS14]: for odd ℓ, secure when

$$q_e \ll 2^{\kappa + \frac{\ell-1}{\ell+1} n}$$

Plain Cascade Encryption

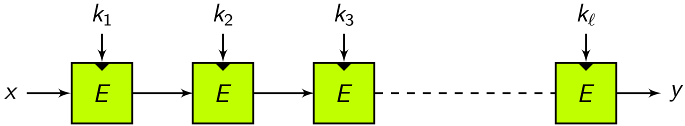


Cascade Encryption

- encrypt ℓ times with independent keys
- $\ell = 2$ does not help (meet-in-the-middle attack [DH77])
- security gain starting from $\ell = 3$ [BR06]
- tight bound for $q_c = 2^n$ [DLMS14]: for odd ℓ, secure when

$$q_e \ll 2^{\kappa + \frac{\ell-1}{\ell+1} n}$$

Plain Cascade Encryption

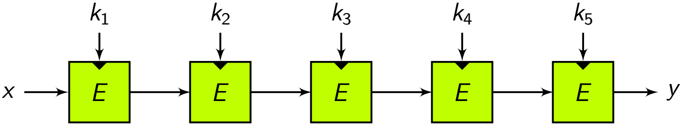


Cascade Encryption

- encrypt ℓ times with independent keys
- $\ell = 2$ does not help (meet-in-the-middle attack [DH77])
- security gain starting from $\ell = 3$ [BR06]
- tight bound for $q_c = 2^n$ [DLMS14]: for odd ℓ, secure when

$$q_e \ll 2^{\kappa + \frac{\ell-1}{\ell+1} n}$$

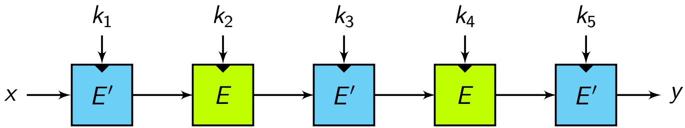
Our Analysis of Plain Cascade Encryption



- use 2 independent ideal ciphers E, E' (key-domain separation)
- reveal function table of E' for free $\Rightarrow$ randomized KLE
- apply the KLE-to-ISC Lemma
- generalize analysis of key-alternating ciphers of [CS14]
- our result: plain cascade of length $\ell = 2r + 1$ is secure when

$$q_c \cdot q_e^r \ll 2^{r(\kappa+n)}, \qquad q_c \ll 2^{\kappa}, \qquad q_e \ll 2^{2\kappa}$$

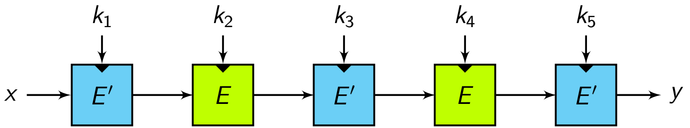
Our Analysis of Plain Cascade Encryption



- use 2 independent ideal ciphers E, E' (key-domain separation)
- reveal function table of E' for free $\Rightarrow$ randomized KLE
- apply the KLE-to-ISC Lemma
- generalize analysis of key-alternating ciphers of [CS14]
- our result: plain cascade of length $\ell = 2r + 1$ is secure when

$$q_c \cdot q_e^r \ll 2^{r(\kappa+n)}, \qquad q_c \ll 2^{\kappa}, \qquad q_e \ll 2^{2\kappa}$$

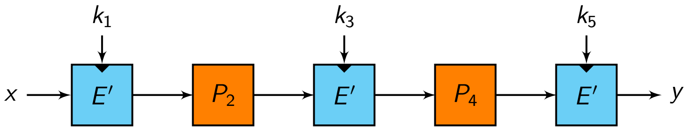
Our Analysis of Plain Cascade Encryption



- use 2 independent ideal ciphers E, E' (key-domain separation)
- reveal function table of E' for free $\Rightarrow$ randomized KLE
- apply the KLE-to-ISC Lemma
- generalize analysis of key-alternating ciphers of [CS14]
- our result: plain cascade of length $\ell = 2r + 1$ is secure when

$$q_c \cdot q_e^r \ll 2^{r(\kappa+n)}, \qquad q_c \ll 2^{\kappa}, \qquad q_e \ll 2^{2\kappa}$$

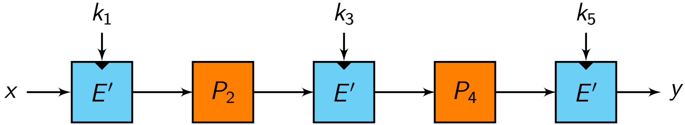
Our Analysis of Plain Cascade Encryption



- use 2 independent ideal ciphers E, E' (key-domain separation)
- reveal function table of E' for free $\Rightarrow$ randomized KLE
- apply the KLE-to-ISC Lemma
- generalize analysis of key-alternating ciphers of [CS14]
- our result: plain cascade of length $\ell = 2r + 1$ is secure when

$$q_c \cdot q_e^r \ll 2^{r(\kappa+n)}, \qquad q_c \ll 2^{\kappa}, \qquad q_e \ll 2^{2\kappa}$$

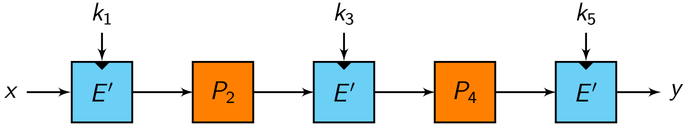
Our Analysis of Plain Cascade Encryption



- use 2 independent ideal ciphers E, E' (key-domain separation)
- reveal function table of E' for free $\Rightarrow$ randomized KLE
- apply the KLE-to-ISC Lemma
- generalize analysis of key-alternating ciphers of [CS14]
- our result: plain cascade of length $\ell = 2r + 1$ is secure when

$$q_c \cdot q_e^r \ll 2^{r(\kappa+n)}, \qquad q_c \ll 2^{\kappa}, \qquad q_e \ll 2^{2\kappa}$$

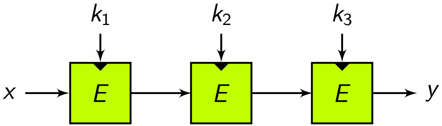
Our Analysis of Plain Cascade Encryption



- use 2 independent ideal ciphers E, E' (key-domain separation)
- reveal function table of E' for free $\Rightarrow$ randomized KLE
- apply the KLE-to-ISC Lemma
- generalize analysis of key-alternating ciphers of [CS14]
- our result: plain cascade of length $\ell = 2r + 1$ is secure when

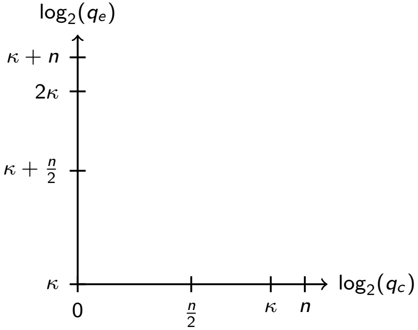
$$q_c \cdot q_e^r \ll 2^{r(\kappa+n)}, \qquad q_c \ll 2^{\kappa}, \qquad q_e \ll 2^{2\kappa}$$

The Case of Triple Encryption



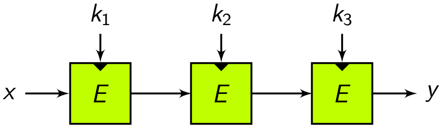
- our bound:

$$q_c \ll 2^{\kappa}$$
$$q_e \ll 2^{2\kappa}$$
$$q_c \cdot q_e \ll 2^{\kappa+n}$$



- when $2^{n/2} \leq q_c \leq 2^n$
  $\Rightarrow$ [DLMS14] bound applies
  $(q_e \ll 2^{\kappa+n/2})$

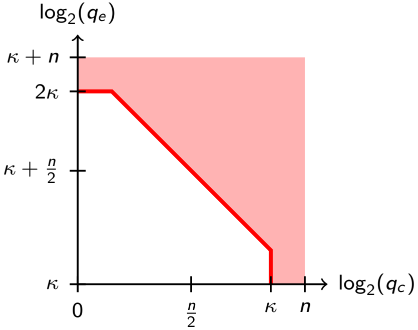
The Case of Triple Encryption



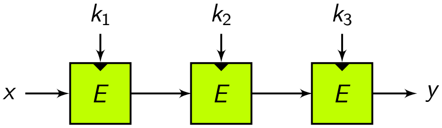
- our bound:

$$q_c \ll 2^{\kappa}$$
$$q_e \ll 2^{2\kappa}$$
$$q_c \cdot q_e \ll 2^{\kappa+n}$$

- when $2^{n/2} \le q_c \le 2^n$
  $\Rightarrow$ [DLMS14] bound applies
  $(q_e \ll 2^{\kappa+n/2})$



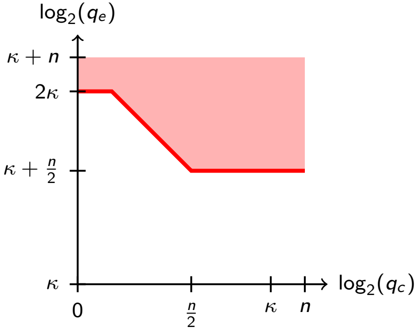
The Case of Triple Encryption



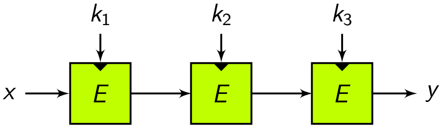
- our bound:

$$q_c \ll 2^{\kappa}$$
$$q_e \ll 2^{2\kappa}$$
$$q_c \cdot q_e \ll 2^{\kappa+n}$$

- when $2^{n/2} \leq q_c \leq 2^n$
  $\Rightarrow$ [DLMS14] bound applies
  $(q_e \ll 2^{\kappa+n/2})$



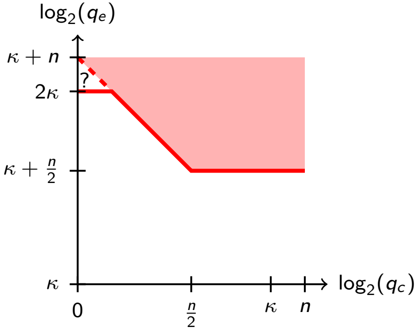
The Case of Triple Encryption



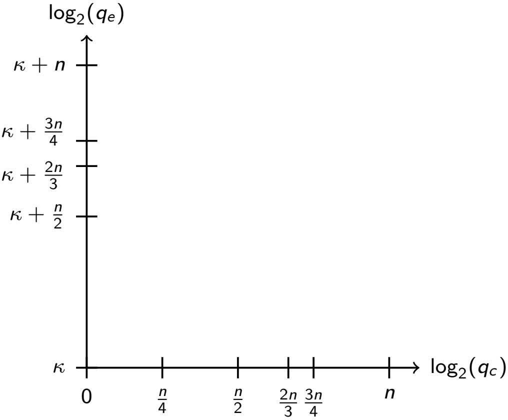
- our bound:

$$q_c \ll 2^{\kappa}$$
$$q_e \ll 2^{2\kappa}$$
$$q_c \cdot q_e \ll 2^{\kappa+n}$$

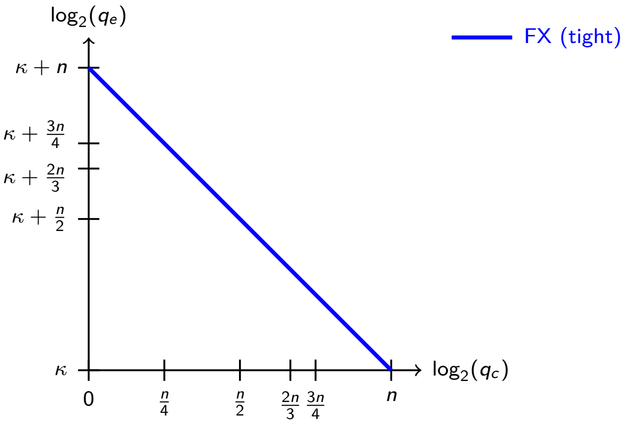
- when $2^{n/2} \leq q_c \leq 2^n$
  $\Rightarrow$ [DLMS14] bound applies
  $(q_e \ll 2^{\kappa+n/2})$



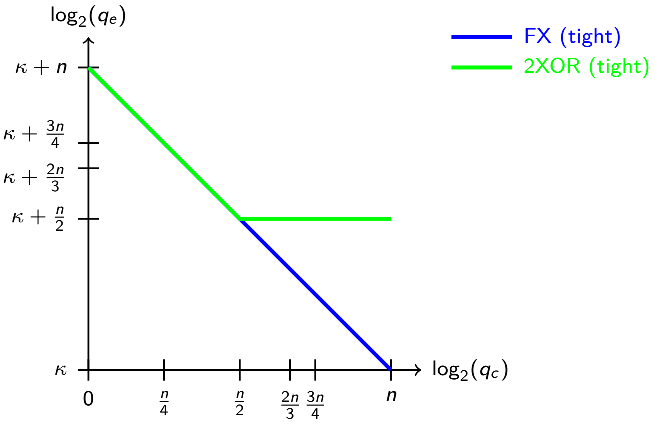
Conclusion I



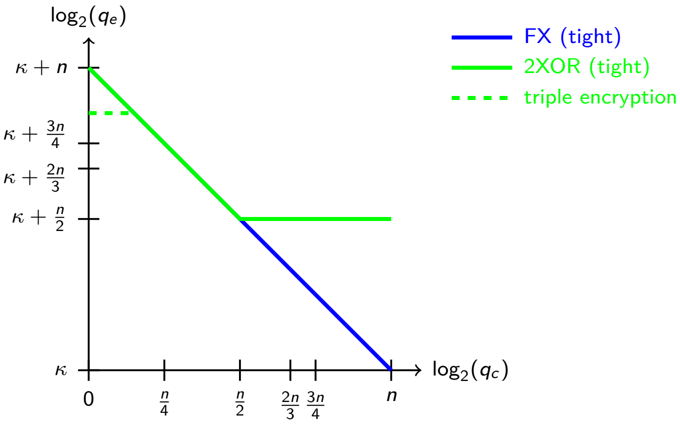
Conclusion I



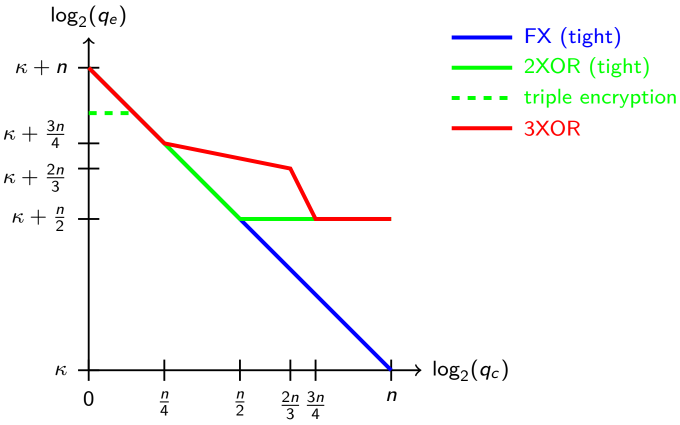
Conclusion I



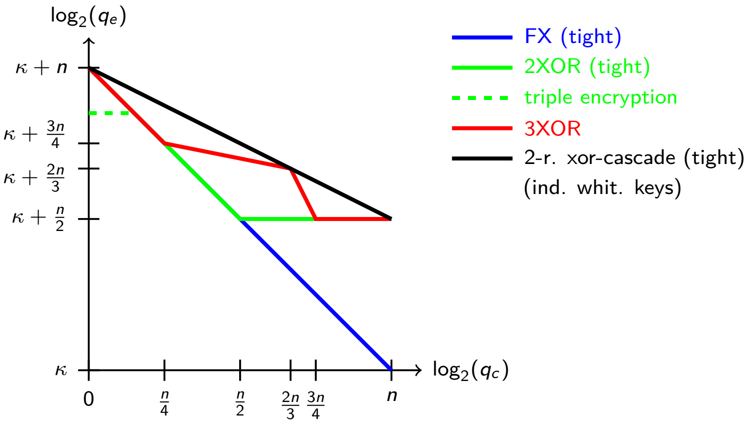
Conclusion I



Conclusion I



Conclusion I



Conclusion II

- our results seem to advocate in favor of xor-cascade rather than plain cascade
- e.g. triple encryption (3 E-calls) has similar security as
  - FX (1 E-call) for $q_c \leq 2^{n/2}$
  - 2XOR (2 E-calls) for $2^{n/2} \leq q_c \leq 2^n$
- but this is in the ideal cipher model (information-theoretic)
- FX seems to have other "computational" issues (see time-memory-data trade-off by Dinur, EC 2015)

Conclusion II

- our results seem to advocate in favor of xor-cascade rather than plain cascade
- e.g. triple encryption (3 E-calls) has similar security as
  - FX (1 E-call) for $q_c \leq 2^{n/2}$
  - 2XOR (2 E-calls) for $2^{n/2} \leq q_c \leq 2^n$
- but this is in the ideal cipher model (information-theoretic)
- FX seems to have other "computational" issues (see time-memory-data trade-off by Dinur, EC 2015)

Conclusion II

- our results seem to advocate in favor of xor-cascade rather than plain cascade
- e.g. triple encryption (3 E-calls) has similar security as
  - FX (1 E-call) for $q_c \leq 2^{n/2}$
  - 2XOR (2 E-calls) for $2^{n/2} \leq q_c \leq 2^n$
- but this is in the ideal cipher model (information-theoretic)
- FX seems to have other "computational" issues (see time-memory-data trade-off by Dinur, EC 2015)

Conclusion II

- our results seem to advocate in favor of xor-cascade rather than plain cascade
- e.g. triple encryption (3 E-calls) has similar security as
  - FX (1 E-call) for $q_c \leq 2^{n/2}$
  - 2XOR (2 E-calls) for $2^{n/2} \leq q_c \leq 2^n$
- but this is in the ideal cipher model (information-theoretic)
- FX seems to have other "computational" issues
  (see time-memory-data trade-off by Dinur, EC 2015)

The end...

Thanks for your attention!

Comments or questions?

References I

Mihir Bellare and Phillip Rogaway. The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 409–426. Springer, 2006. Full version available at `http://eprint.iacr.org/2004/331`.

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`.

References II

- Yuanxi Dai, Jooyoung Lee, Bart Mennink, and John P. Steinberger. The Security of Multiple Encryption in the Ideal Cipher Model. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 (Proceedings, Part I)*, volume 8616 of *LNCS*, pages 20–38. Springer, 2014.
- Peter Gazi. Plain versus Randomized Cascading-Based Key-Length Extension for Block Ciphers. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 (Proceedings, Part I)*, volume 8042 of *LNCS*, pages 551–570. Springer, 2013.
- Peter Gazi and Stefano Tessaro. Efficient and Optimally Secure Key-Length Extension for Block Ciphers via Randomized Cascading. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 63–80. Springer, 2012.
- Joe Kilian and Phillip Rogaway. How to Protect DES Against Exhaustive Key Search (an Analysis of DESX). *Journal of Cryptology*, 14(1):17–35, 2001.