Constructing Tweakable Block Ciphers in the Random Permutation Model

Yannick Seurin

ANSSI, France

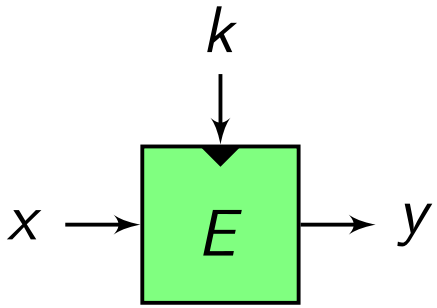
September 30, 2015 — ASK 2015

Based on joint work with Benoît Cogliati and Rodolphe Lampe

Outline

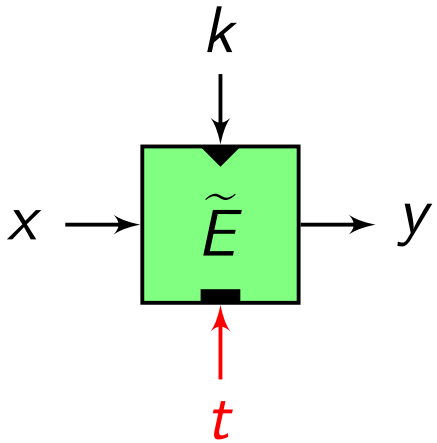
Outline

Tweakable Block Ciphers (TBCs)



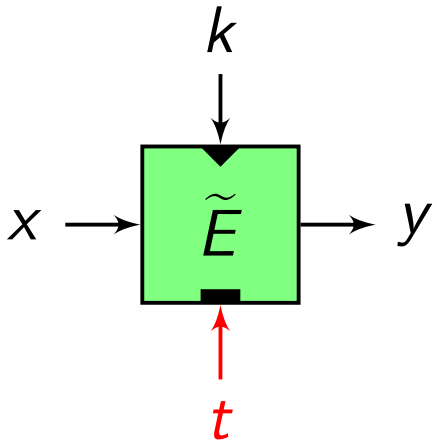
- tweak t: brings variability to the block cipher
- t assumed public or even adversarially controlled
- each tweak should give an "independent" permutation
- few "natively tweakable" BCs:
  - Hasty Pudding Cipher [Sch98]
  - Mercy [Cro00]
  - Threefish [FLS+10]
  - CAESAR proposals KIASU, Deoxys, Joltik, (i)SCREAM, Minalpher

Tweakable Block Ciphers (TBCs)



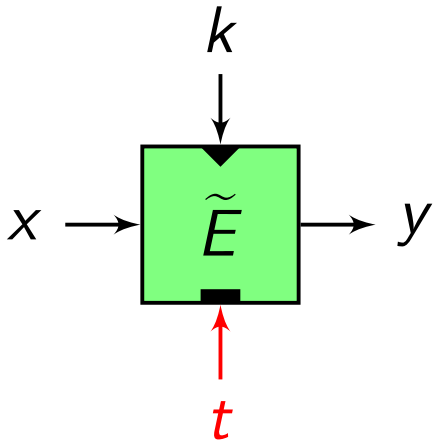
- tweak t: brings variability to the block cipher
- t assumed public or even adversarially controlled
- each tweak should give an "independent" permutation
- few "natively tweakable" BCs:
  - Hasty Pudding Cipher [Sch98]
  - Mercy [Cro00]
  - Threefish [FLS+10]
  - CAESAR proposals KIASU, Deoxys, Joltik, (i)SCREAM, Minalpher

Tweakable Block Ciphers (TBCs)



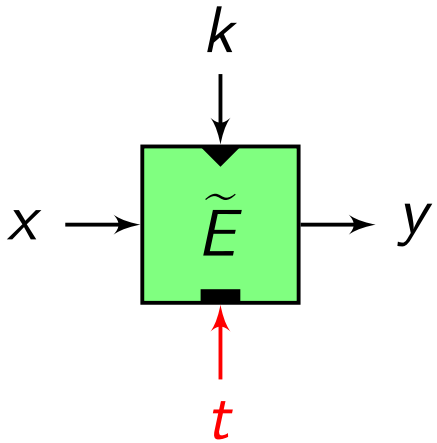
- tweak t: brings variability to the block cipher
- t assumed public or even adversarially controlled
- each tweak should give an "independent" permutation
- few "natively tweakable" BCs:
  - Hasty Pudding Cipher [Sch98]
  - Mercy [Cro00]
  - Threefish [FLS+10]
  - CAESAR proposals KIASU, Deoxys, Joltik, (i)SCREAM, Minalpher

Tweakable Block Ciphers (TBCs)



- tweak t: brings variability to the block cipher
- t assumed public or even adversarially controlled
- each tweak should give an "independent" permutation
- few "natively tweakable" BCs:
  - Hasty Pudding Cipher [Sch98]
  - Mercy [Cro00]
  - Threefish [FLS+10]
  - CAESAR proposals KIASU, Deoxys, Joltik, (i)SCREAM, Minalpher

Tweakable Block Ciphers (TBCs)



- tweak t: brings variability to the block cipher
- t assumed public or even adversarially controlled
- each tweak should give an "independent" permutation
- few "natively tweakable" BCs:
  - Hasty Pudding Cipher [Sch98]
  - Mercy [Cro00]
  - Threefish [FLS+10]
  - CAESAR proposals KIASU, Deoxys, Joltik, (i)SCREAM, Minalpher

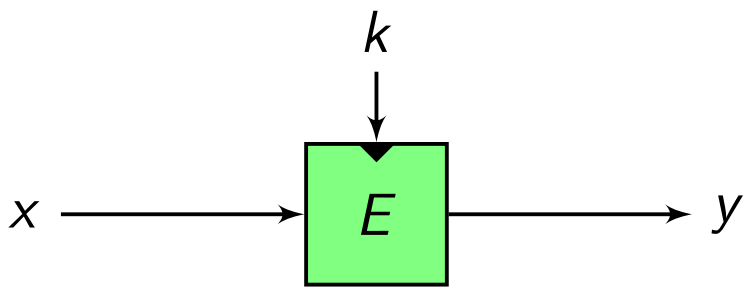
Generic Constructions of TBCs: LRW

- A generic TBC construction turns a conventional block cipher E into a TBC $\widetilde{E}$
- example: LRW construction by Liskov *et al.* [LRW02]

- h is XOR-universal, e.g. $h_{k'}(t) = k' \otimes t$ (field mult.)
- secure up to $\sim 2^{n/2}$ queries
- related construction XEX [Rog04] uses $E_k(t)$ instead of $h_{k'}(t)$ (used e.g. in the XTS disk encryption mode)

Generic Constructions of TBCs: LRW

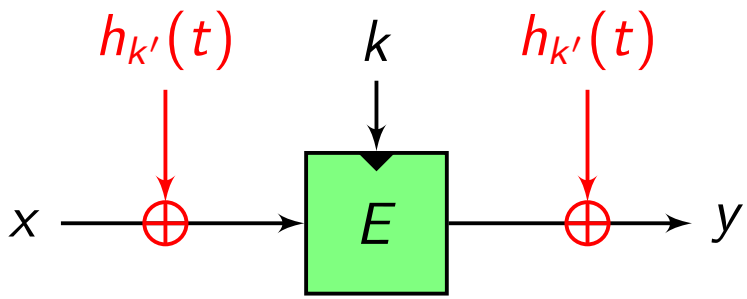
- A generic TBC construction turns a conventional block cipher E into a TBC $\widetilde{E}$
- example: LRW construction by Liskov *et al.* [LRW02]



- h is XOR-universal, e.g. $h_{k'}(t) = k' \otimes t$ (field mult.)
- secure up to $\sim 2^{n/2}$ queries
- related construction XEX [Rog04] uses $E_k(t)$ instead of $h_{k'}(t)$ (used e.g. in the XTS disk encryption mode)

Generic Constructions of TBCs: LRW

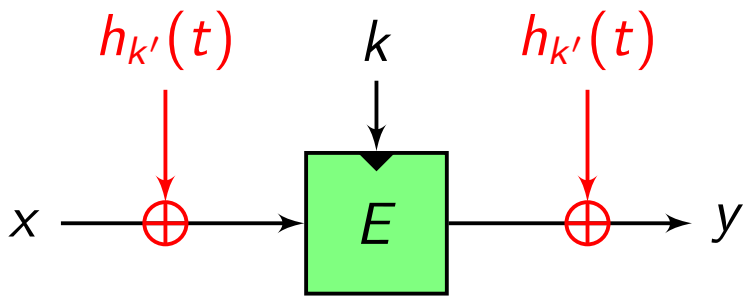
- A generic TBC construction turns a conventional block cipher E into a TBC $\widetilde{E}$
- example: LRW construction by Liskov *et al.* [LRW02]



- h is XOR-universal, e.g. $h_{k'}(t) = k' \otimes t$ (field mult.)
- secure up to $\sim 2^{n/2}$ queries
- related construction XEX [Rog04] uses $E_k(t)$ instead of $h_{k'}(t)$ (used e.g. in the XTS disk encryption mode)

Generic Constructions of TBCs: LRW

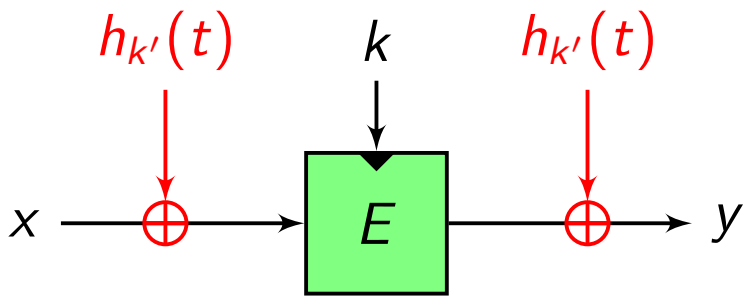
- A generic TBC construction turns a conventional block cipher E into a TBC $\widetilde{E}$
- example: LRW construction by Liskov *et al.* [LRW02]



- h is XOR-universal, e.g. $h_{k'}(t) = k' \otimes t$ (field mult.)
- secure up to $\sim 2^{n/2}$ queries
- related construction XEX [Rog04] uses $E_k(t)$ instead of $h_{k'}(t)$ (used e.g. in the XTS disk encryption mode)

Generic Constructions of TBCs: LRW

- A generic TBC construction turns a conventional block cipher E into a TBC $\widetilde{E}$
- example: LRW construction by Liskov *et al.* [LRW02]



- h is XOR-universal, e.g. $h_{k'}(t) = k' \otimes t$ (field mult.)
- secure up to $\sim 2^{n/2}$ queries
- related construction XEX [Rog04] uses $E_k(t)$ instead of $h_{k'}(t)$ (used e.g. in the XTS disk encryption mode)

Other Generic Constructions

Constructions achieving beyond-birthday-bound security:

- Minematsu [Min09]
  ☹ tweak length $< n/2$
- Cascaded LRW [LST12, LS13]
  ☹ larger key length and block cipher calls
- Mennink [Men15]
  ☹ security proof needs ideal cipher model

Only LRW (or rather XEX) is used in practice (e.g. in the XTS disk encryption mode)

Other Generic Constructions

Constructions achieving beyond-birthday-bound security:

- Minematsu [Min09]
  ☹ tweak length $< n/2$
- Cascaded LRW [LST12, LS13]
  ☹ larger key length and block cipher calls
- Mennink [Men15]
  ☹ security proof needs ideal cipher model

Only LRW (or rather XEX) is used in practice (e.g. in the XTS disk encryption mode)

Other Generic Constructions

Constructions achieving beyond-birthday-bound security:

- Minematsu [Min09]
  ☹ tweak length $< n/2$
- Cascaded LRW [LST12, LS13]
  ☹ larger key length and block cipher calls
- Mennink [Men15]
  ☹ security proof needs ideal cipher model

Only LRW (or rather XEX) is used in practice (e.g. in the XTS disk encryption mode)

Other Generic Constructions

Constructions achieving beyond-birthday-bound security:

- Minematsu [Min09]
  ☹ tweak length $< n/2$
- Cascaded LRW [LST12, LS13]
  ☹ larger key length and block cipher calls
- Mennink [Men15]
  ☹ security proof needs ideal cipher model

Only LRW (or rather XEX) is used in practice (e.g. in the XTS disk encryption mode)

Other Generic Constructions

Constructions achieving beyond-birthday-bound security:

- Minematsu [Min09]
  ☹ tweak length $< n/2$
- Cascaded LRW [LST12, LS13]
  ☹ larger key length and block cipher calls
- Mennink [Men15]
  ☹ security proof needs ideal cipher model

Only LRW (or rather XEX) is used in practice (e.g. in the XTS disk encryption mode)

Outline

TBCs: Dedicated Designs

Our Goal

Provide provable security guidelines to design TBCs "from scratch" (rather than from an existing conventional block cipher).

- "from scratch" $\rightarrow$ from some lower level primitive
- from a PRF: Feistel schemes [GHL+07, MI08]
- this talk: SPN ciphers (more gen. key-alternating ciphers)

TBCs: Dedicated Designs

Our Goal

Provide provable security guidelines to design TBCs "from scratch" (rather than from an existing conventional block cipher).

- "from scratch" $\rightarrow$ from some lower level primitive
- from a PRF: Feistel schemes [GHL+07, MI08]
- this talk: SPN ciphers (more gen. key-alternating ciphers)

TBCs: Dedicated Designs

Our Goal

Provide provable security guidelines to design TBCs "from scratch" (rather than from an existing conventional block cipher).

- "from scratch" $\rightarrow$ from some lower level primitive
- from a PRF: Feistel schemes [GHL$^+$07, MI08]
- this talk: SPN ciphers (more gen. key-alternating ciphers)

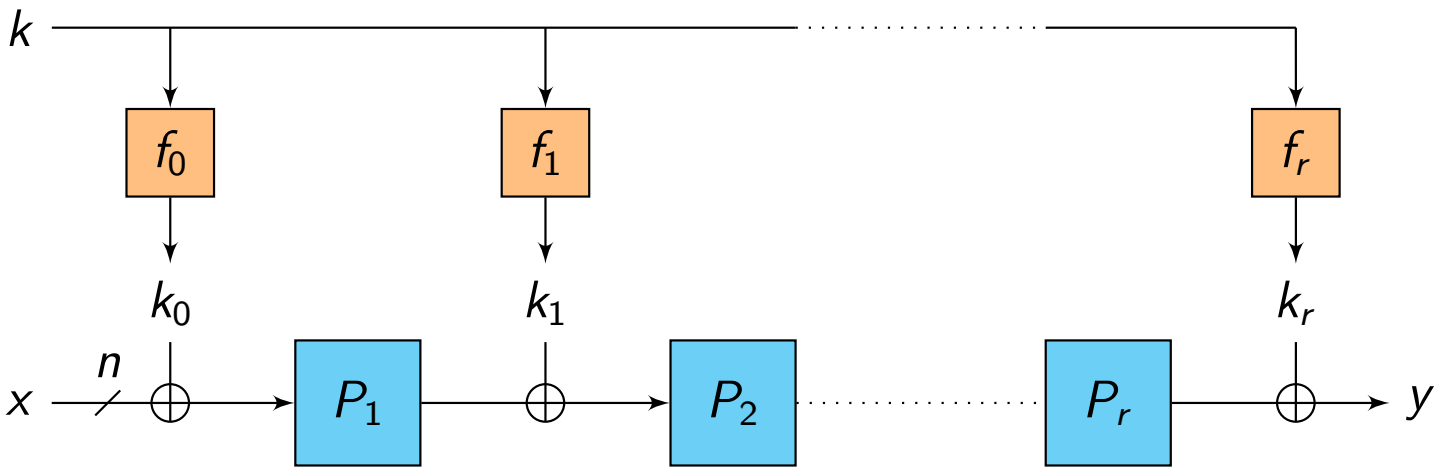
TBCs: Dedicated Designs

Our Goal

Provide provable security guidelines to design TBCs "from scratch" (rather than from an existing conventional block cipher).

- "from scratch" $\rightarrow$ from some lower level primitive
- from a PRF: Feistel schemes [GHL$^+$07, MI08]
- this talk: SPN ciphers (more gen. key-alternating ciphers)

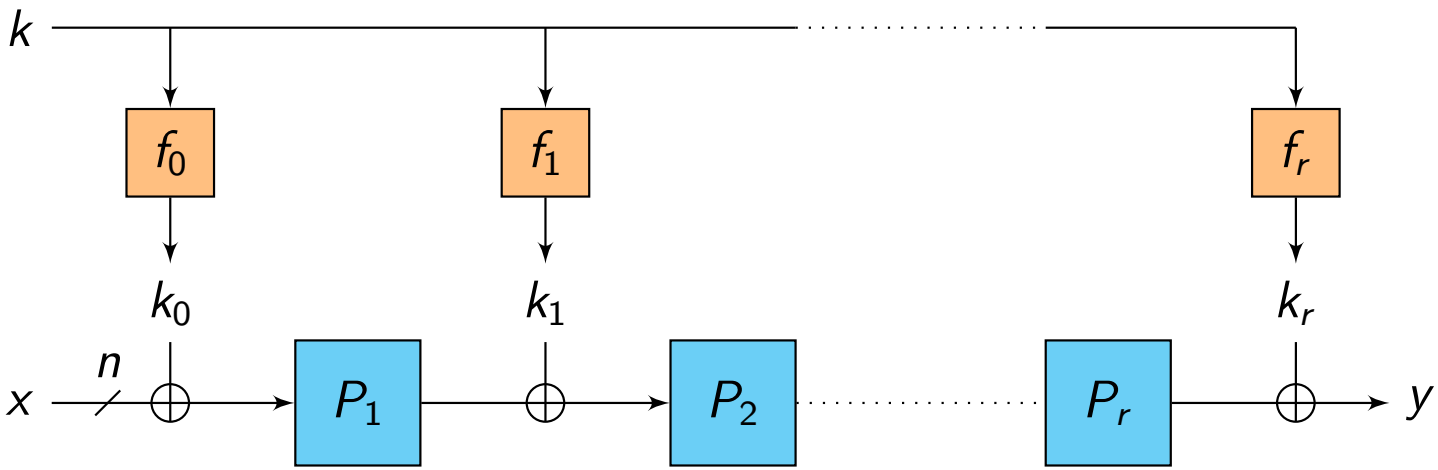
Key-Alternating Ciphers



An r-round key-alternating cipher:

- the P_i's are public permutations on $\{0,1\}^n$
- the f_i's map k to n-bit "round keys"
- examples: most SPNs (AES, SERPENT, PRESENT, LED...)
- a.k.a. (iterated) Even-Mansour construction

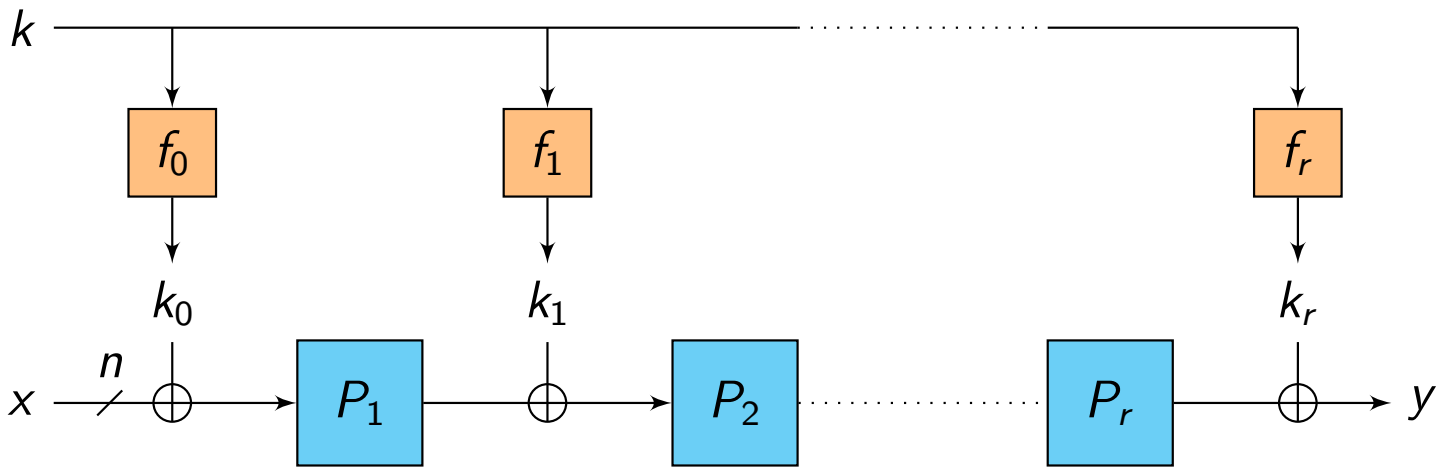
Key-Alternating Ciphers



An r-round key-alternating cipher:

- the P_i's are public permutations on $\{0,1\}^n$
- the f_i's map k to n-bit "round keys"
- examples: most SPNs (AES, SERPENT, PRESENT, LED...)
- a.k.a. (iterated) Even-Mansour construction

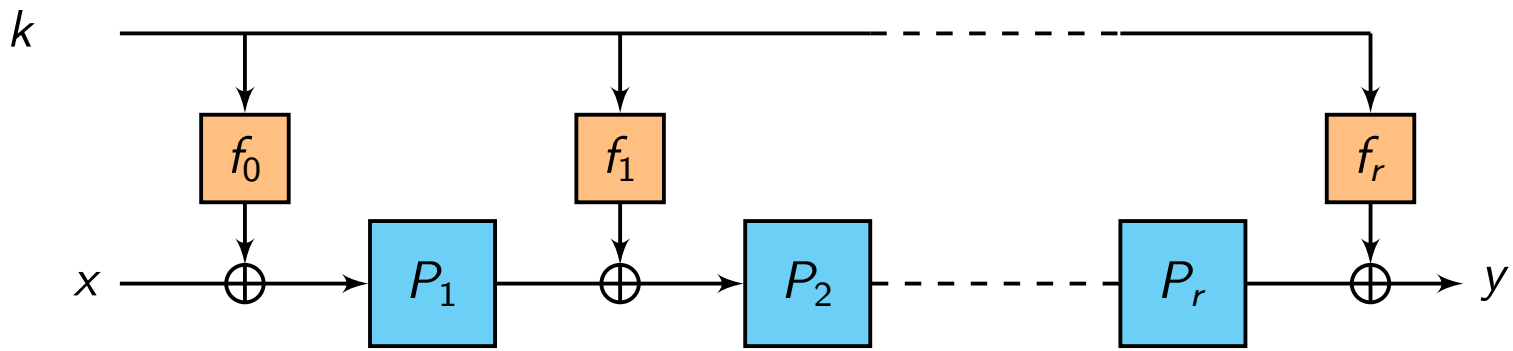
Key-Alternating Ciphers



An r-round key-alternating cipher:

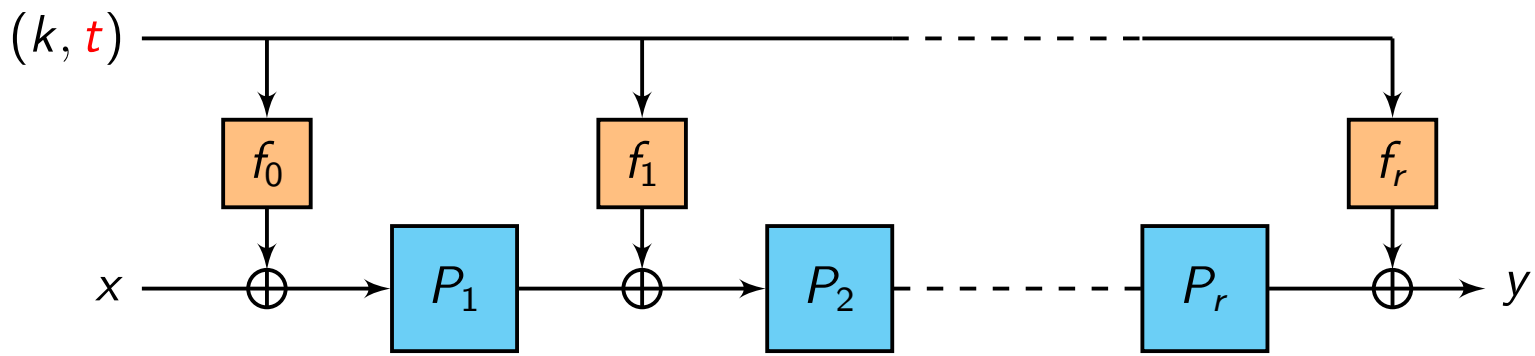
- the P_i's are public permutations on $\{0,1\}^n$
- the f_i's map k to n-bit "round keys"
- examples: most SPNs (AES, SERPENT, PRESENT, LED...)
- a.k.a. (iterated) Even-Mansour construction

Tweakable Even-Mansour Constructions



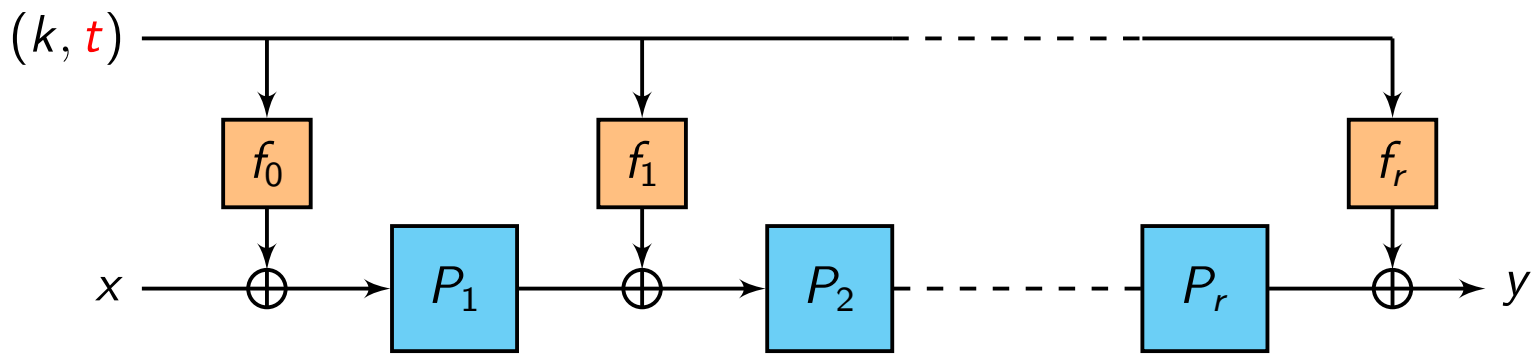
- let the round keys depend on the key and the tweak t
- $\Rightarrow$ "tweakable" Even-Mansour (TEM) construction(s)
- f_i's = "tweak and key schedule" (TKS)
- high-level abstraction of the TWEAKEY constructions [JNP14]
- analysis in the Random Permutation Model

Tweakable Even-Mansour Constructions



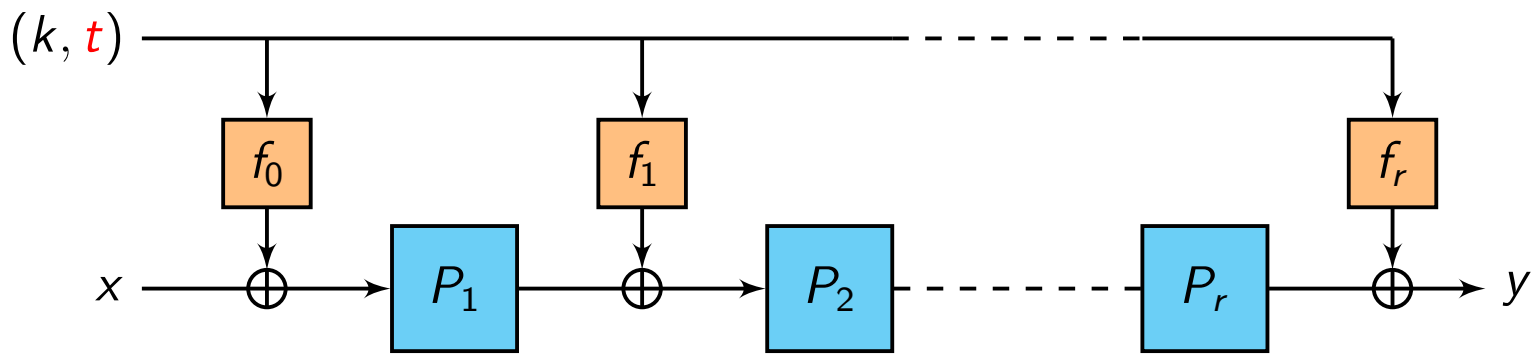
- let the round keys depend on the key and the tweak t
- $\Rightarrow$ "tweakable" Even-Mansour (TEM) construction(s)
- f_i's = "tweak and key schedule" (TKS)
- high-level abstraction of the TWEAKEY constructions [JNP14]
- analysis in the Random Permutation Model

Tweakable Even-Mansour Constructions



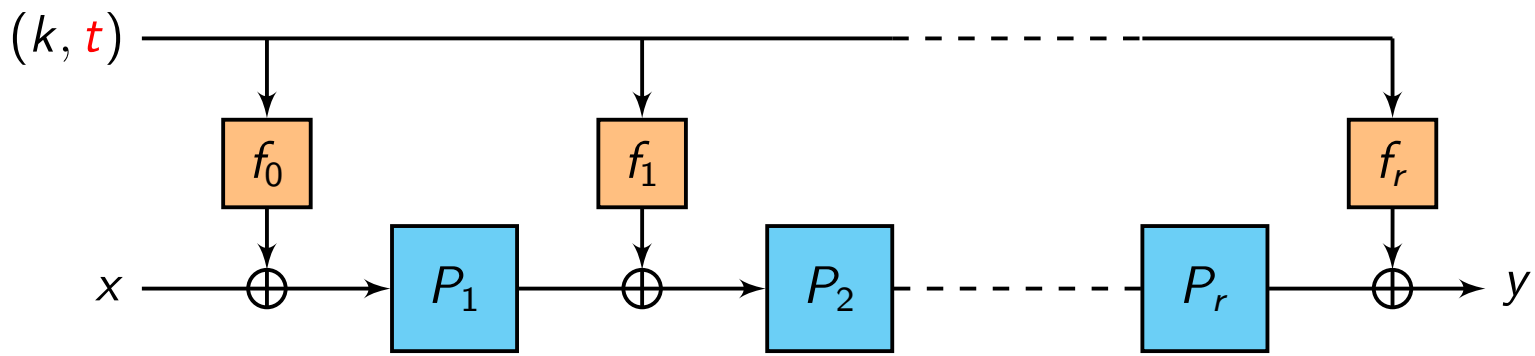
- let the round keys depend on the key and the tweak t
- $\Rightarrow$ "tweakable" Even-Mansour (TEM) construction(s)
- f_i's = "tweak and key schedule" (TKS)
- high-level abstraction of the TWEAKEY constructions [JNP14]
- analysis in the Random Permutation Model

Tweakable Even-Mansour Constructions



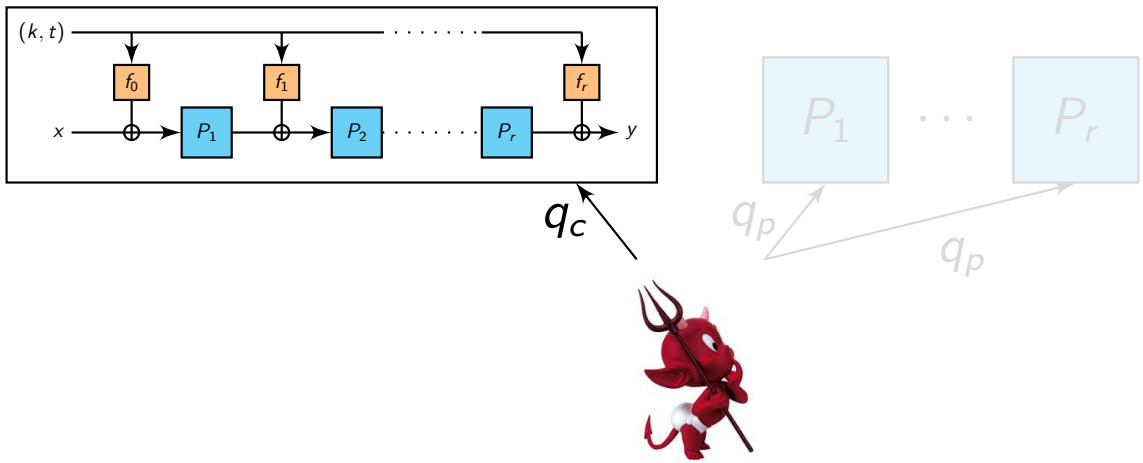
- let the round keys depend on the key and the tweak t
- $\Rightarrow$ "tweakable" Even-Mansour (TEM) construction(s)
- f_i's = "tweak and key schedule" (TKS)
- high-level abstraction of the TWEAKEY constructions [JNP14]
- analysis in the Random Permutation Model

Tweakable Even-Mansour Constructions



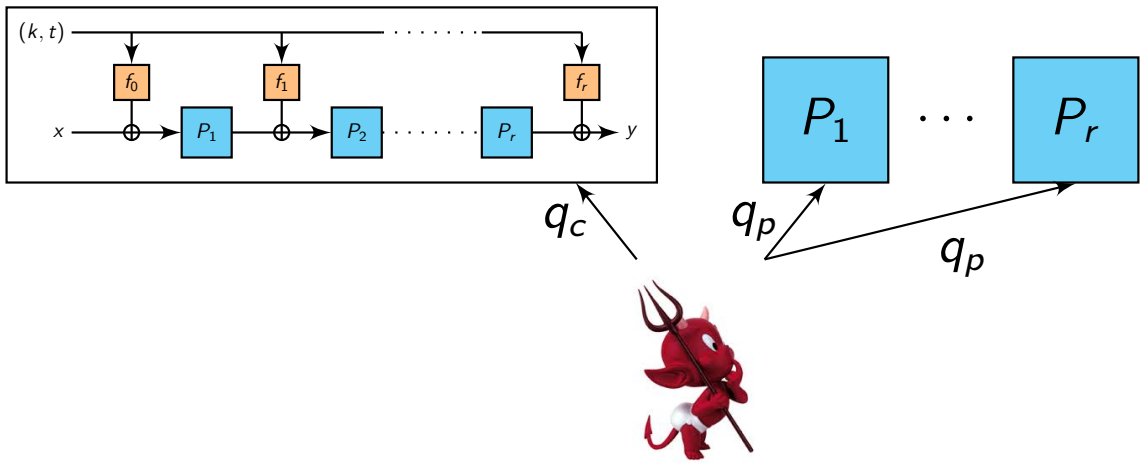
- let the round keys depend on the key and the tweak t
- $\Rightarrow$ "tweakable" Even-Mansour (TEM) construction(s)
- f_i's = "tweak and key schedule" (TKS)
- high-level abstraction of the TWEAKEY constructions [JNP14]
- analysis in the Random Permutation Model

The Random Permutation Model (RPM)



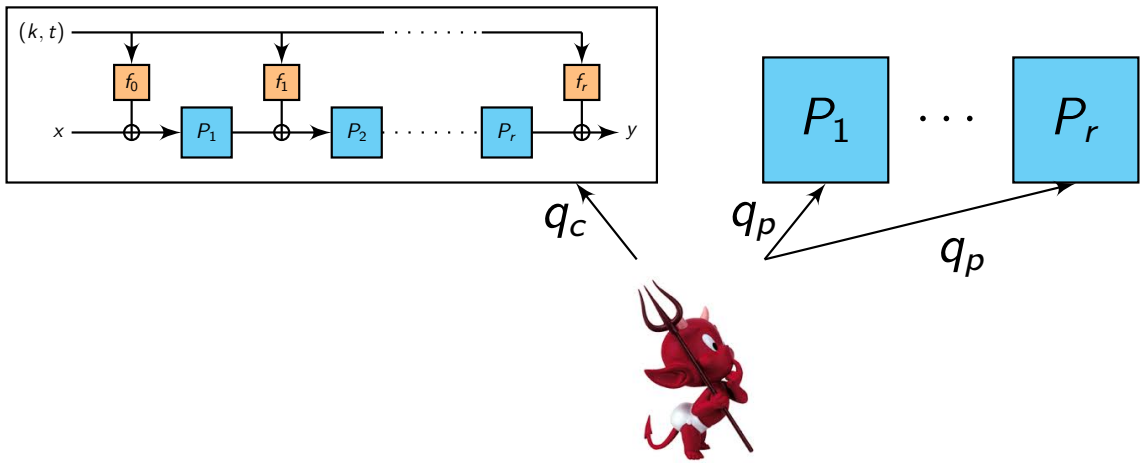
- the P_i's are modeled as public random permutation oracles (adversary can only make black-box queries)
- adversary cannot exploit any weakness of the P_i's
  $\Rightarrow$ generic attacks
- complexity measure of the adversary:
  - q_c = # construction queries = pt/ct pairs (data D)
  - q_p = # queries to each internal permutation oracle (time T)
  - but otherwise computationally unbounded
- $\Rightarrow$ information-theoretic proof of security

The Random Permutation Model (RPM)



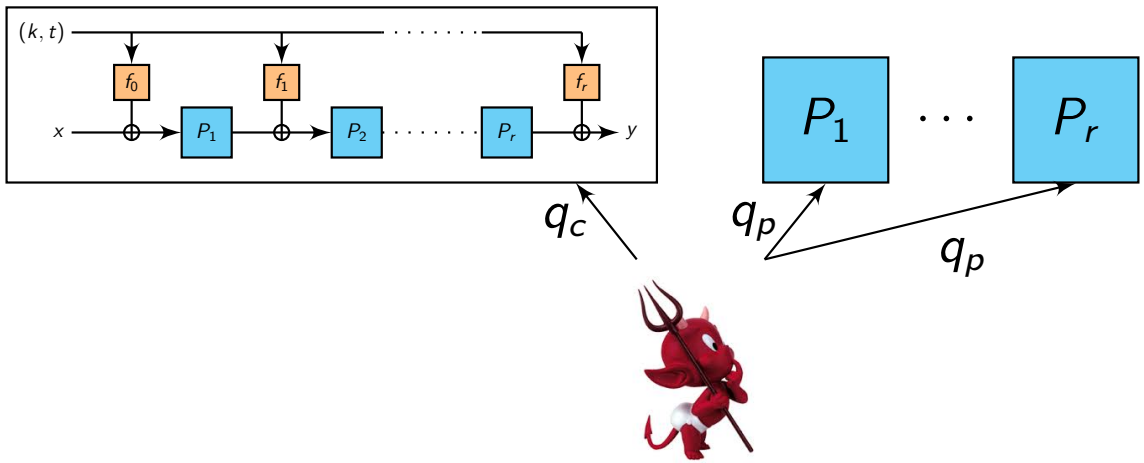
- the P_i's are modeled as public random permutation oracles (adversary can only make black-box queries)
- adversary cannot exploit any weakness of the P_i's
  $\Rightarrow$ generic attacks
- complexity measure of the adversary:
  - $q_c = \#$ construction queries $=$ pt/ct pairs (data D)
  - $q_p = \#$ queries to each internal permutation oracle (time T)
  - but otherwise computationally unbounded
- $\Rightarrow$ information-theoretic proof of security

The Random Permutation Model (RPM)



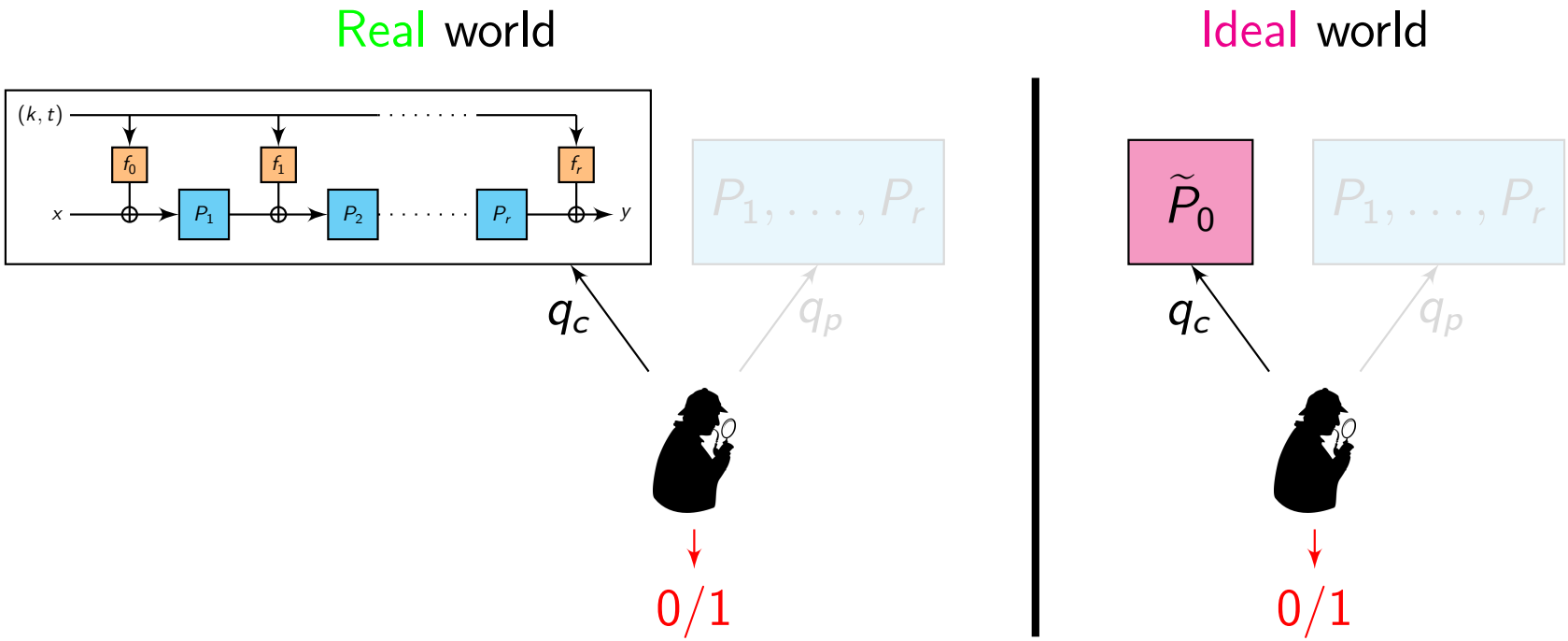
- the P_i's are modeled as public random permutation oracles (adversary can only make black-box queries)
- adversary cannot exploit any weakness of the P_i's
  $\Rightarrow$ generic attacks
- complexity measure of the adversary:
  - $q_c = \#$ construction queries $=$ pt/ct pairs (data D)
  - $q_p = \#$ queries to each internal permutation oracle (time T)
  - but otherwise computationally unbounded
- $\Rightarrow$ information-theoretic proof of security

The Random Permutation Model (RPM)



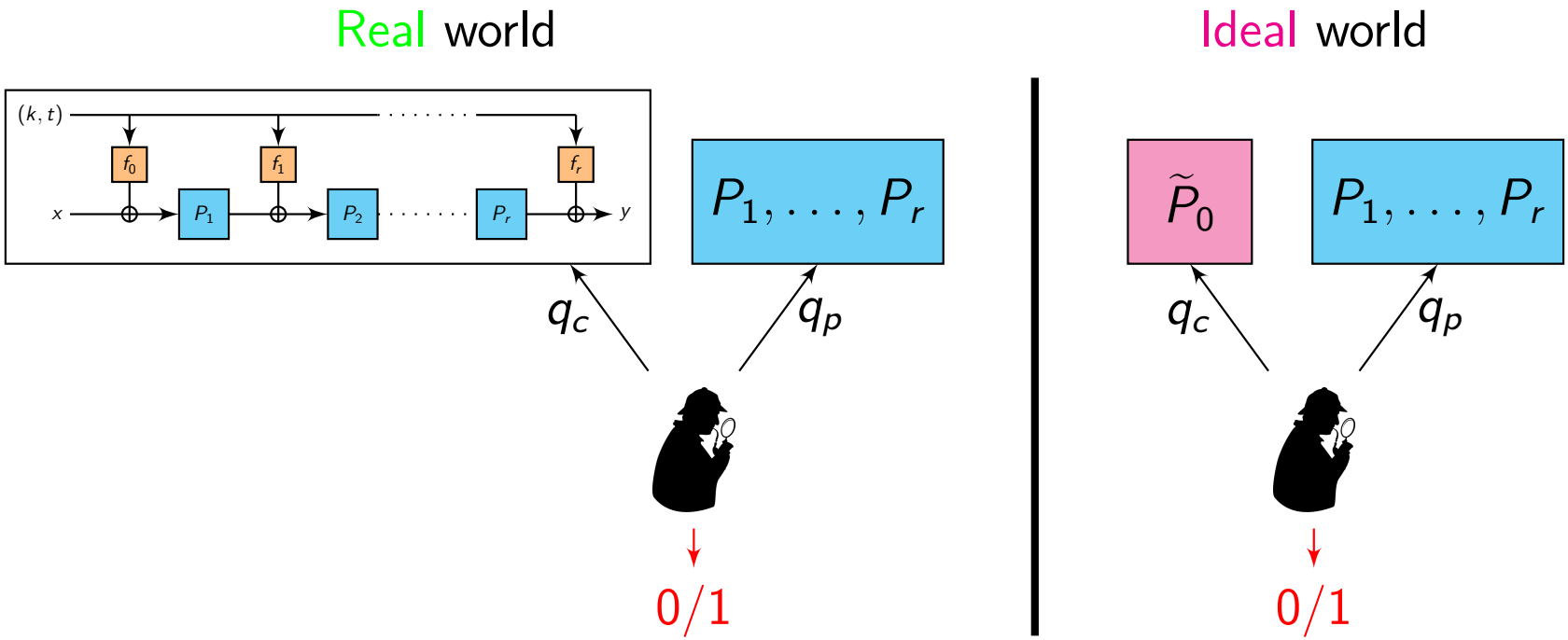
- the P_i's are modeled as public random permutation oracles (adversary can only make black-box queries)
- adversary cannot exploit any weakness of the P_i's
  $\Rightarrow$ generic attacks
- complexity measure of the adversary:
  - $q_c = \#$ construction queries $=$ pt/ct pairs (data D)
  - $q_p = \#$ queries to each internal permutation oracle (time T)
  - but otherwise computationally unbounded
- $\Rightarrow$ information-theoretic proof of security

Formalization of the Security Experiment



- real world: TEM construction with random master key k
- ideal world: random tweakable permutation $\widetilde{P}_0$ independent from $P_1, \ldots, P_r$
- RPM: $\mathcal{D}$ has oracle access to $P_1, \ldots, P_r$ in both worlds

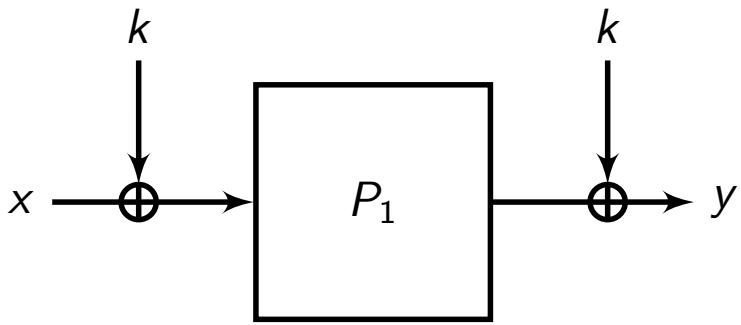
Formalization of the Security Experiment



- real world: TEM construction with random master key k
- ideal world: random tweakable permutation $\widetilde{P}_0$ independent from $P_1, \ldots, P_r$
- RPM: $\mathcal{D}$ has oracle access to $P_1, \ldots, P_r$ in both worlds

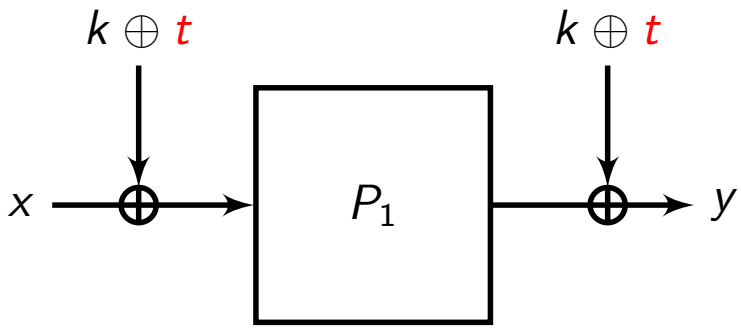
Outline

First Try: One Round, Linear TKS



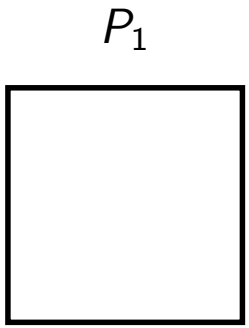
- 2 queries to the encryption oracle, 0 queries to P_1
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

First Try: One Round, Linear TKS



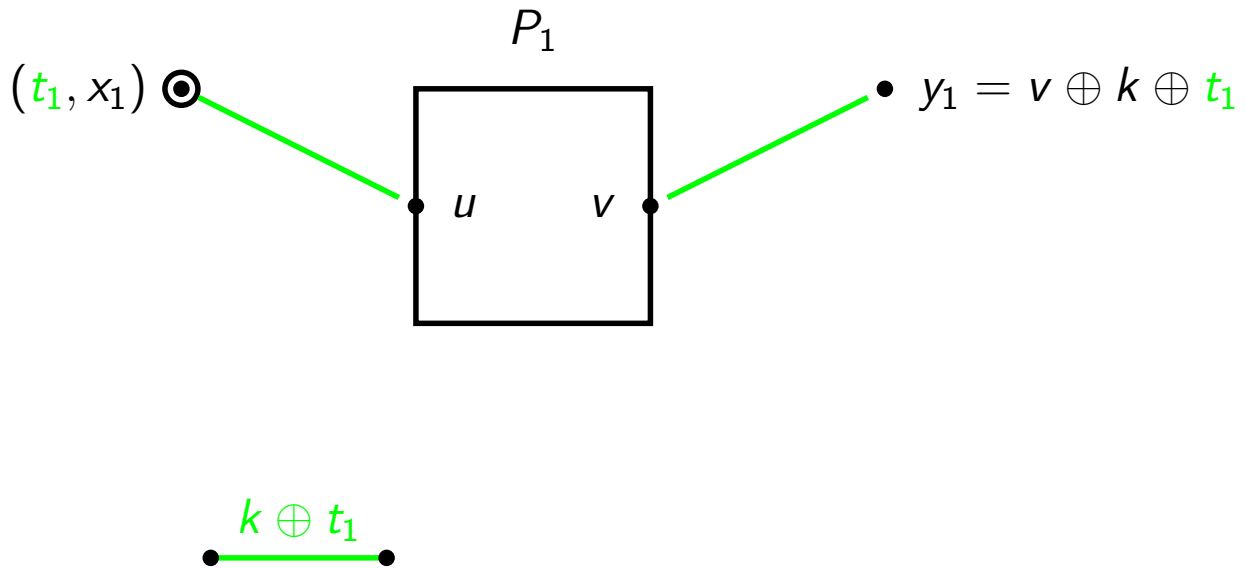
- 2 queries to the encryption oracle, 0 queries to P_1
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

First Try: One Round, Linear TKS



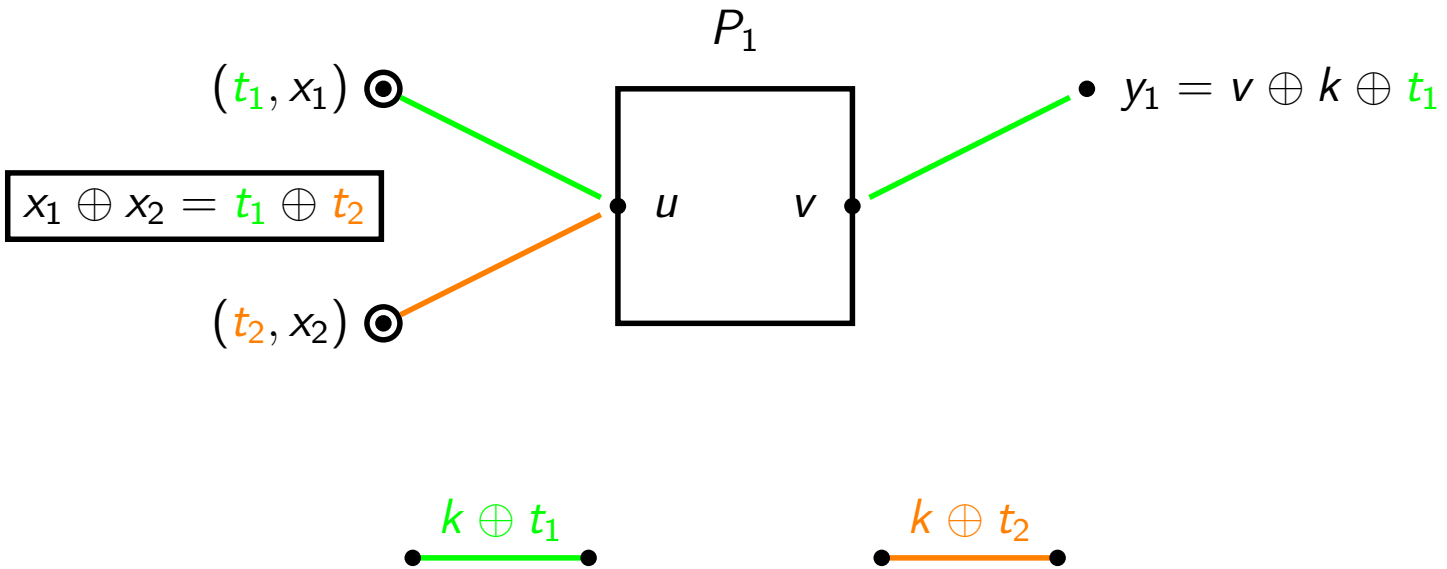
- 2 queries to the encryption oracle, 0 queries to P_1
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

First Try: One Round, Linear TKS



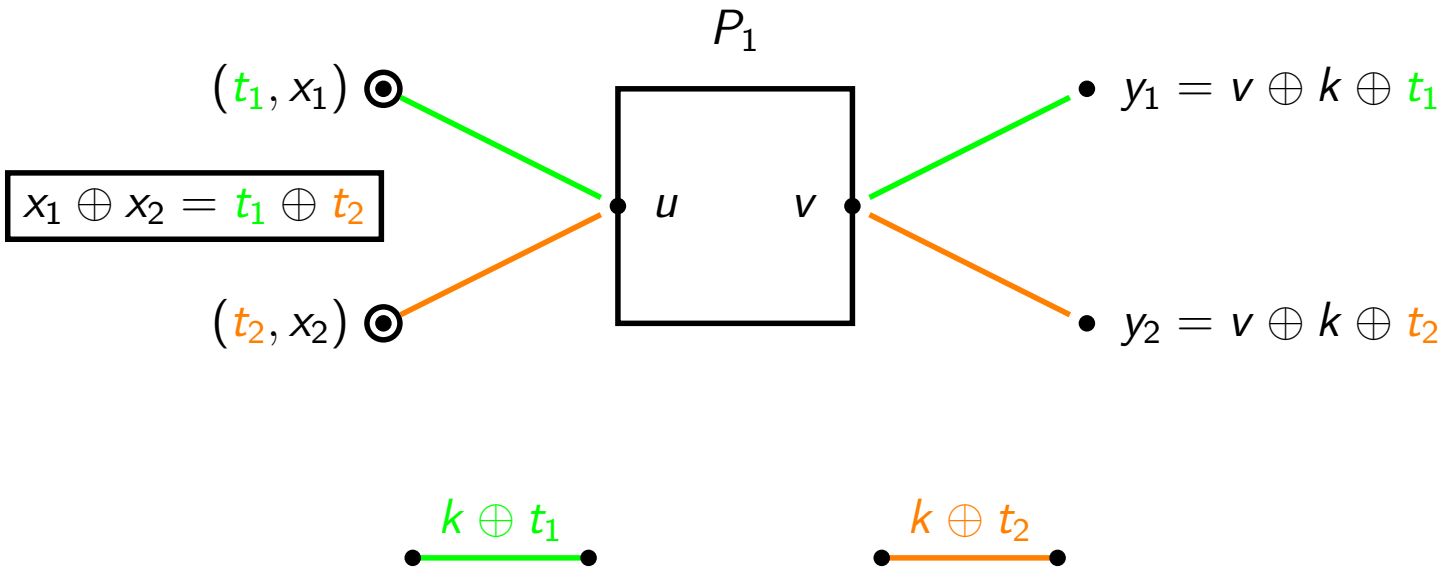
- 2 queries to the encryption oracle, 0 queries to P_1
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

First Try: One Round, Linear TKS



- 2 queries to the encryption oracle, 0 queries to P_1
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

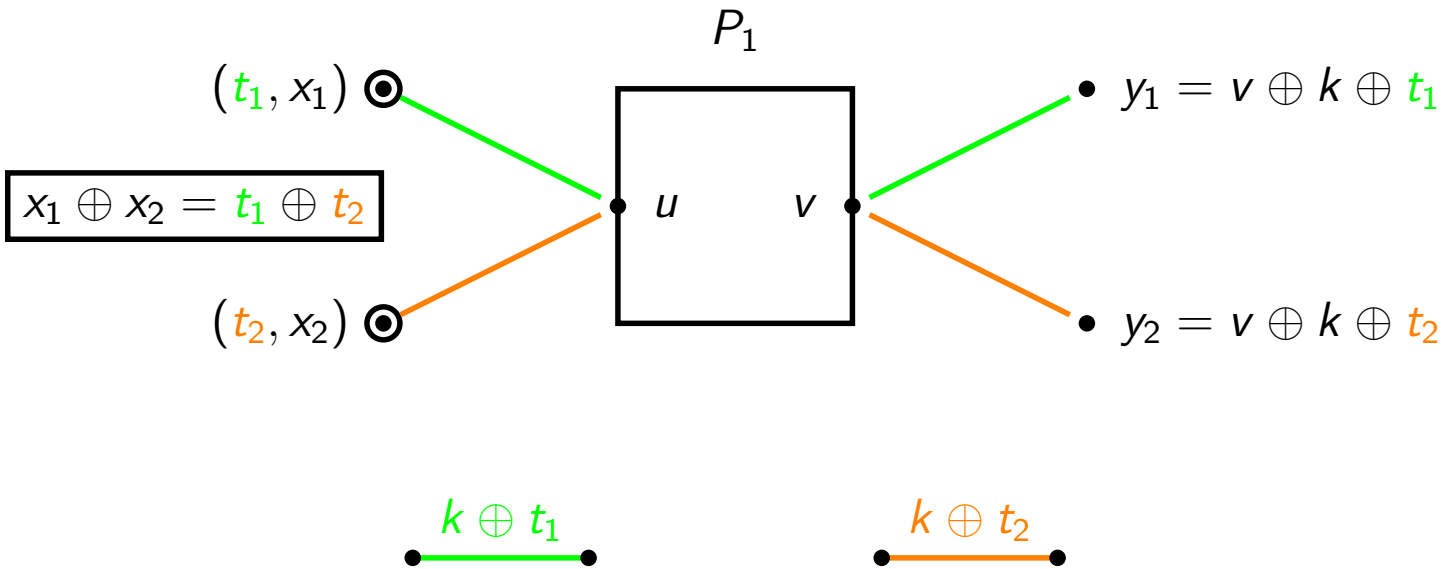
First Try: One Round, Linear TKS



Check that $y_1 \oplus y_2 = t_1 \oplus t_2$ $(*)$

- 2 queries to the encryption oracle, 0 queries to P_1
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

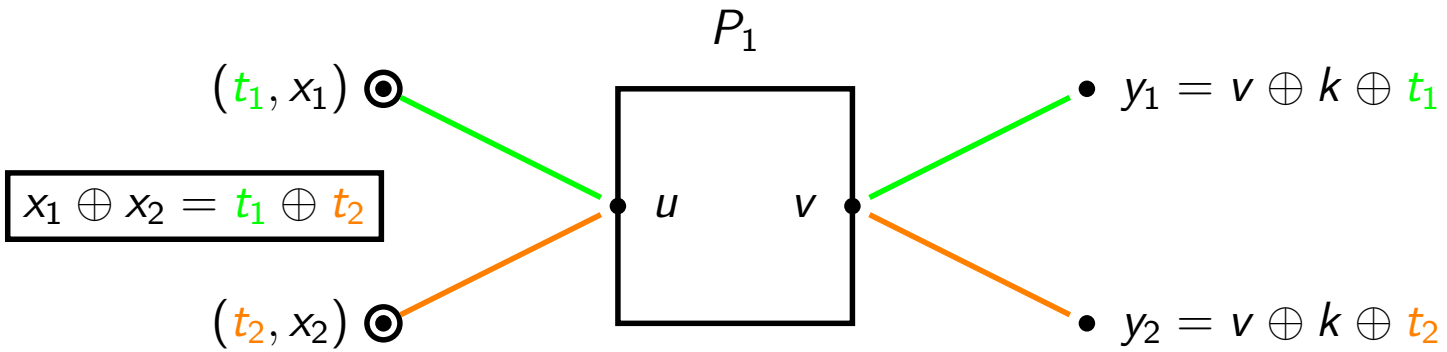
First Try: One Round, Linear TKS



Check that $y_1 \oplus y_2 = t_1 \oplus t_2$ $(*)$

- 2 queries to the encryption oracle, 0 queries to P_1
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

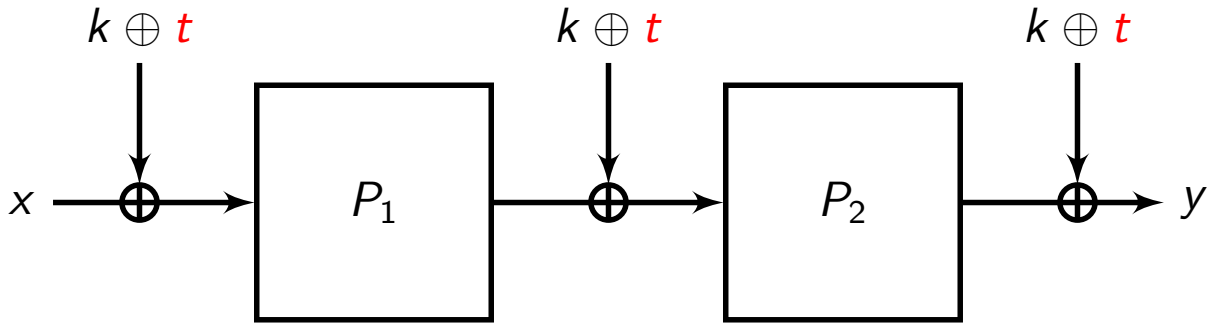
First Try: One Round, Linear TKS



Check that $y_1 \oplus y_2 = t_1 \oplus t_2$ $(*)$

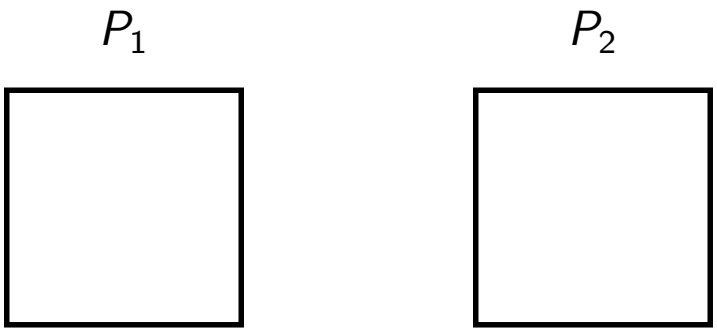
- 2 queries to the encryption oracle, 0 queries to P_1
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

Second Try: Two Rounds, Linear TKS



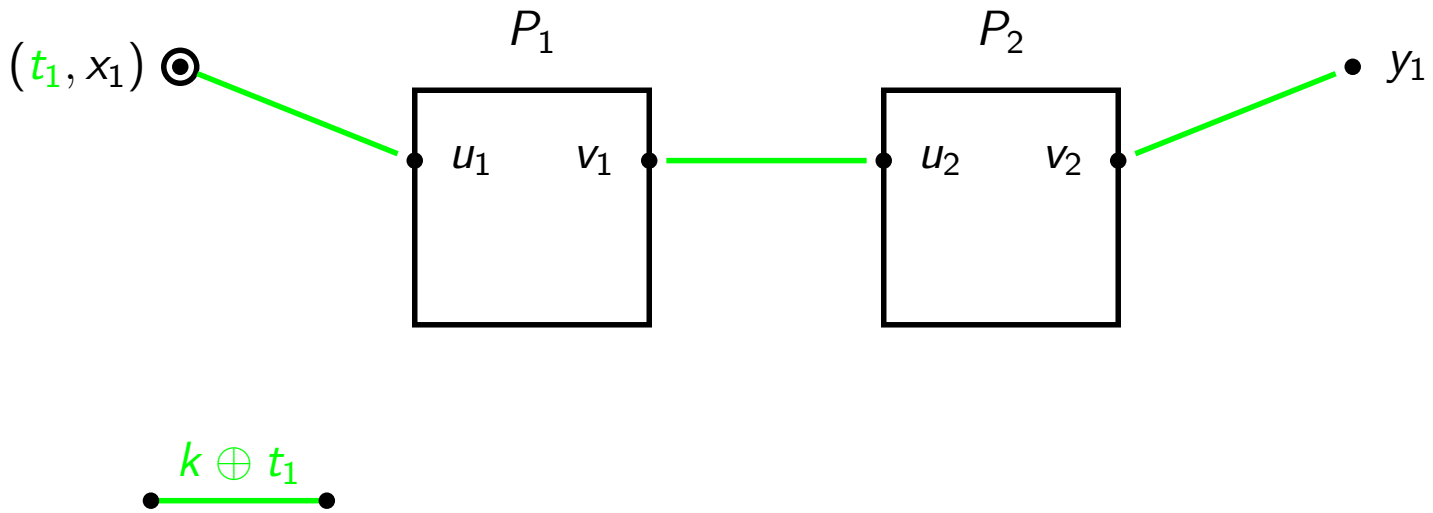
- 4 queries to the enc/dec oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

Second Try: Two Rounds, Linear TKS



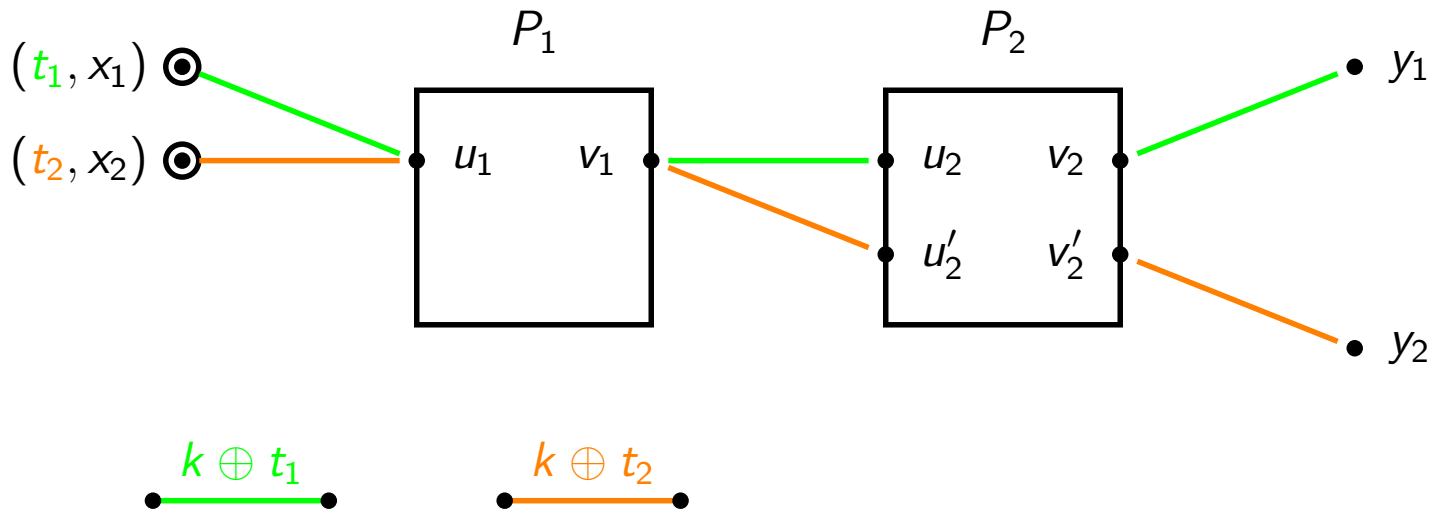
- 4 queries to the enc/dec oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

Second Try: Two Rounds, Linear TKS



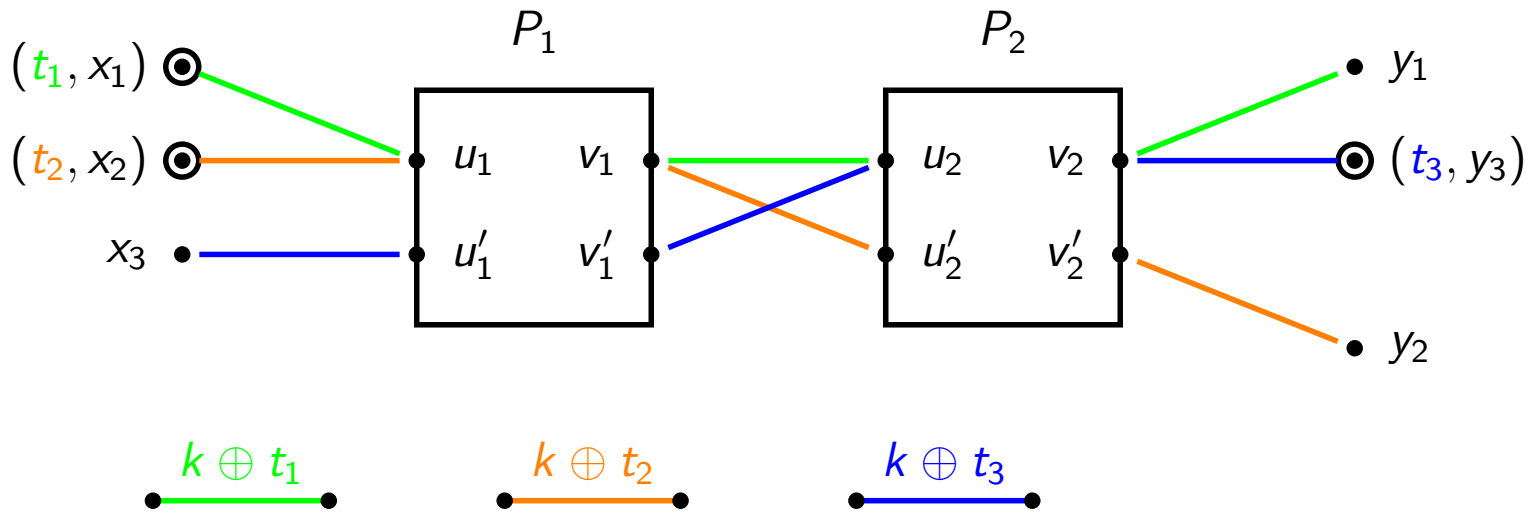
- 4 queries to the enc/dec oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

Second Try: Two Rounds, Linear TKS



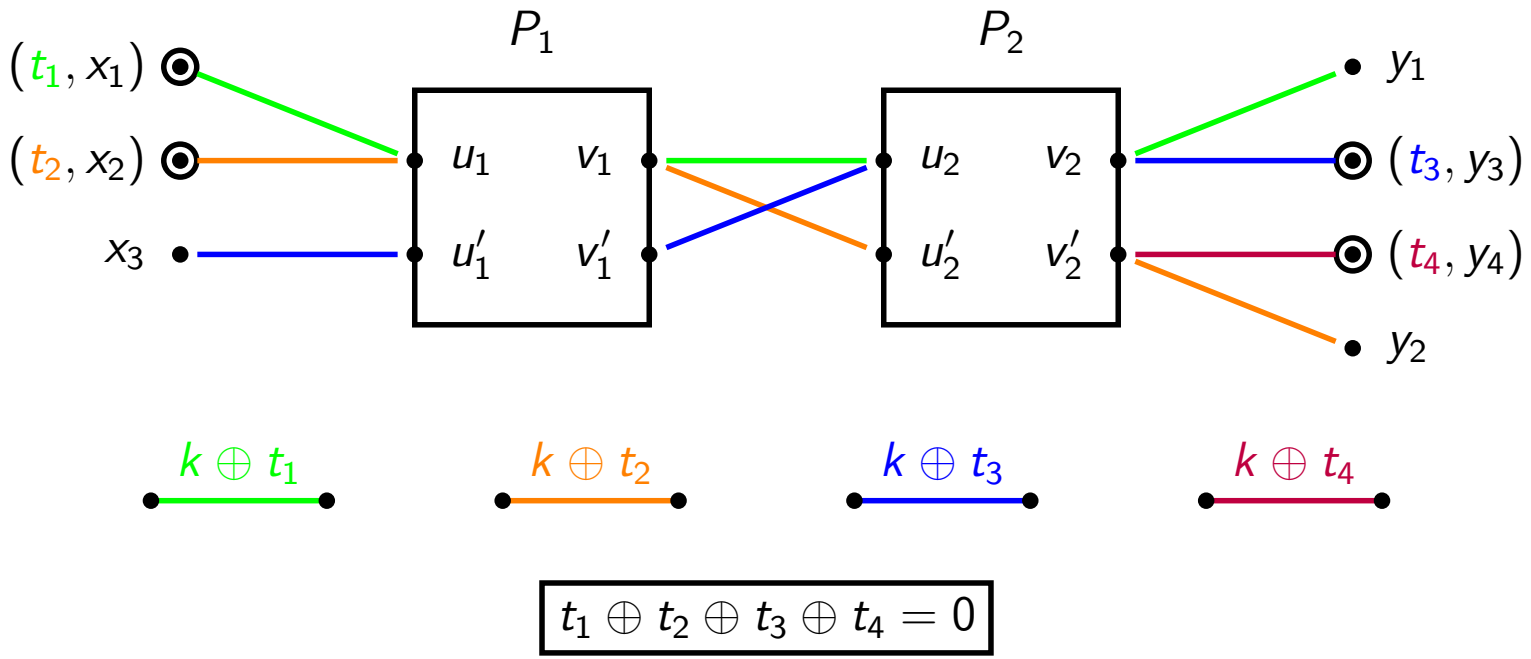
- 4 queries to the enc/dec oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

Second Try: Two Rounds, Linear TKS



- 4 queries to the enc/dec oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

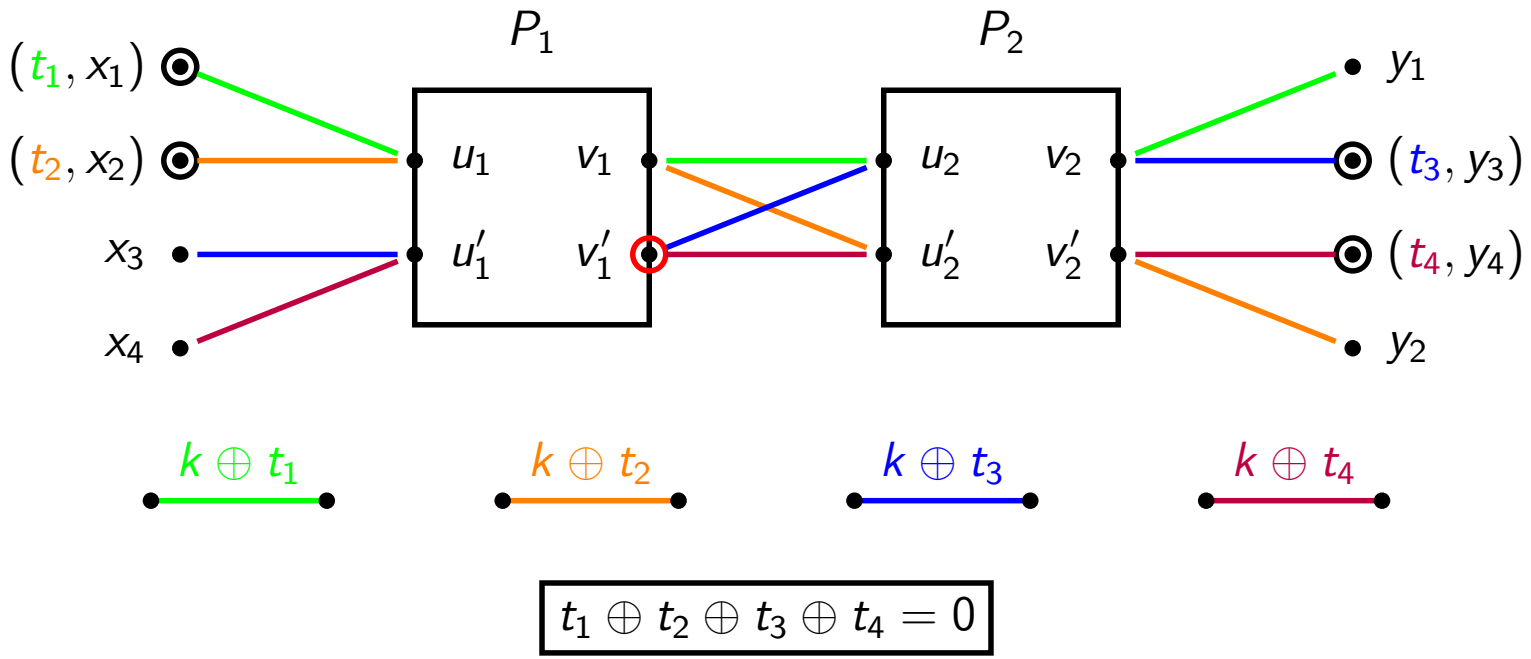
Second Try: Two Rounds, Linear TKS



$$t_1 \oplus t_2 \oplus t_3 \oplus t_4 = 0$$

- 4 queries to the enc/dec oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

Second Try: Two Rounds, Linear TKS

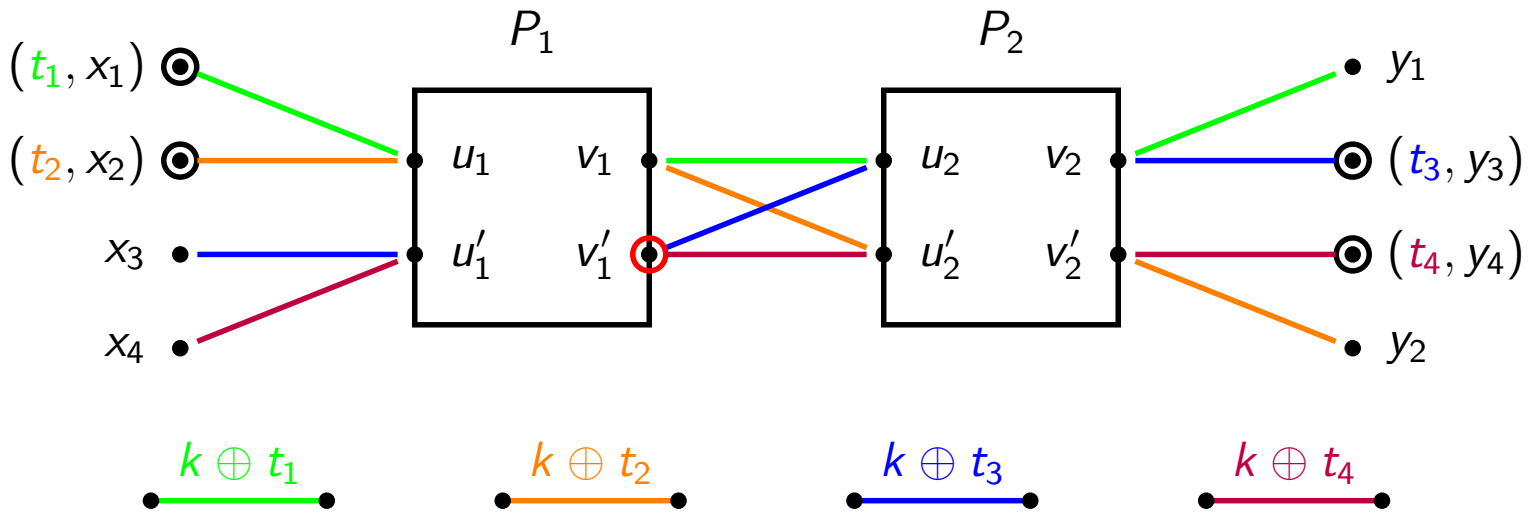


$$t_1 \oplus t_2 \oplus t_3 \oplus t_4 = 0$$

Check that $x_3 \oplus x_4 = t_3 \oplus t_4$ $(*)$

- 4 queries to the enc/dec oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

Second Try: Two Rounds, Linear TKS

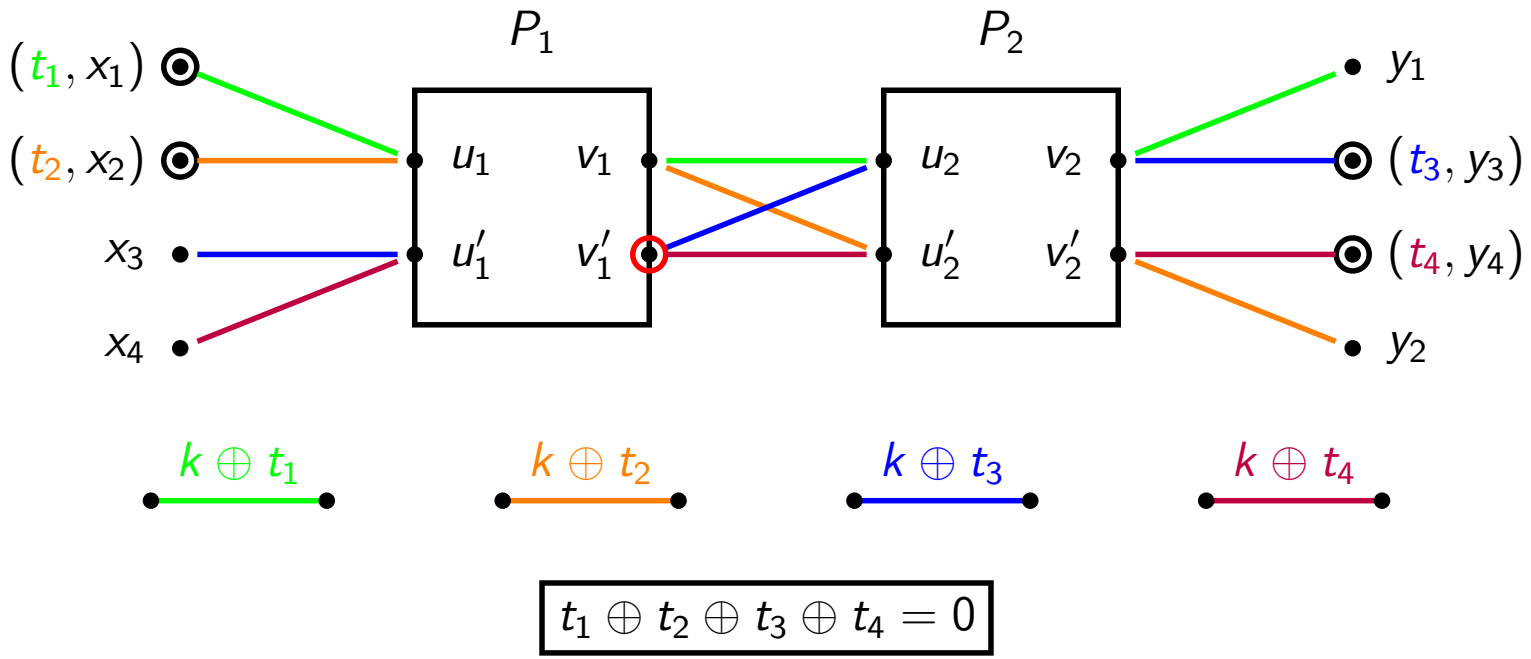


$$t_1 \oplus t_2 \oplus t_3 \oplus t_4 = 0$$

Check that $x_3 \oplus x_4 = t_3 \oplus t_4$ $(*)$

- 4 queries to the enc/dec oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

Second Try: Two Rounds, Linear TKS

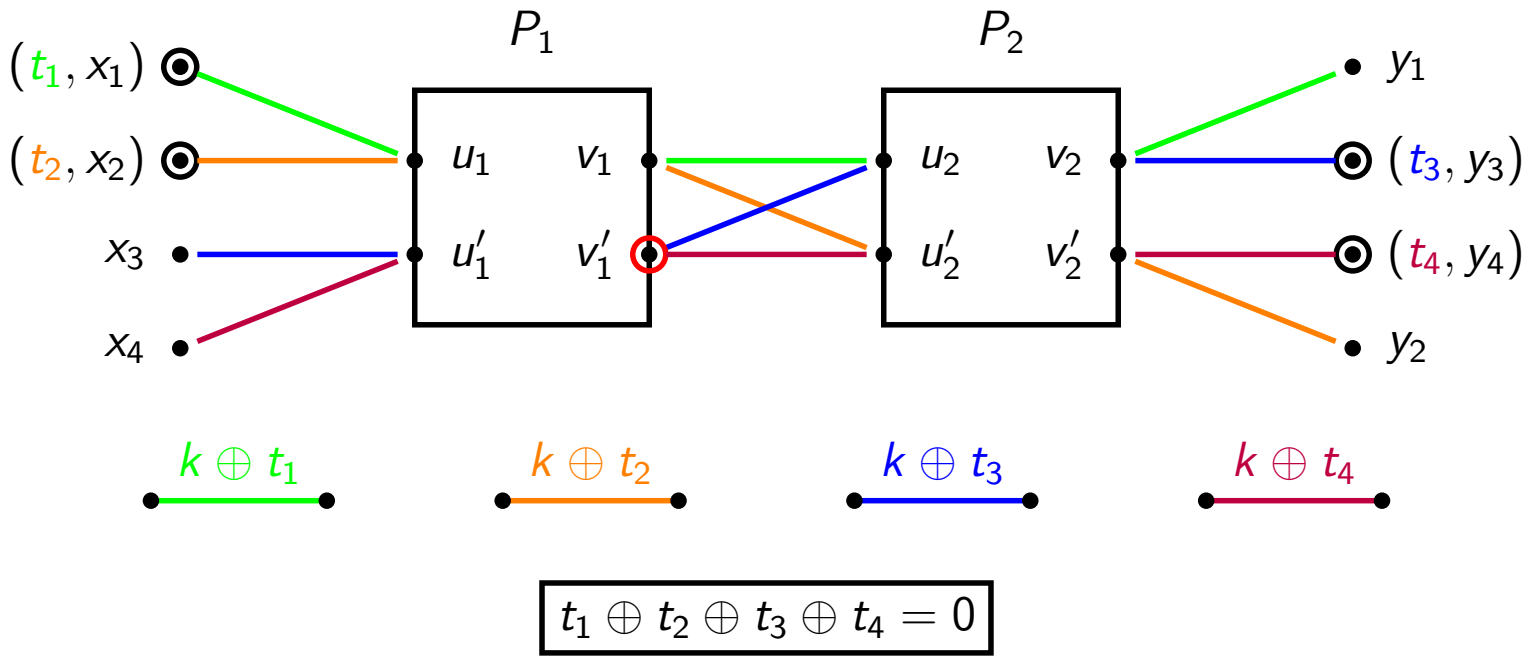


$$t_1 \oplus t_2 \oplus t_3 \oplus t_4 = 0$$

Check that $x_3 \oplus x_4 = t_3 \oplus t_4$ $(*)$

- 4 queries to the enc/dec oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

Second Try: Two Rounds, Linear TKS

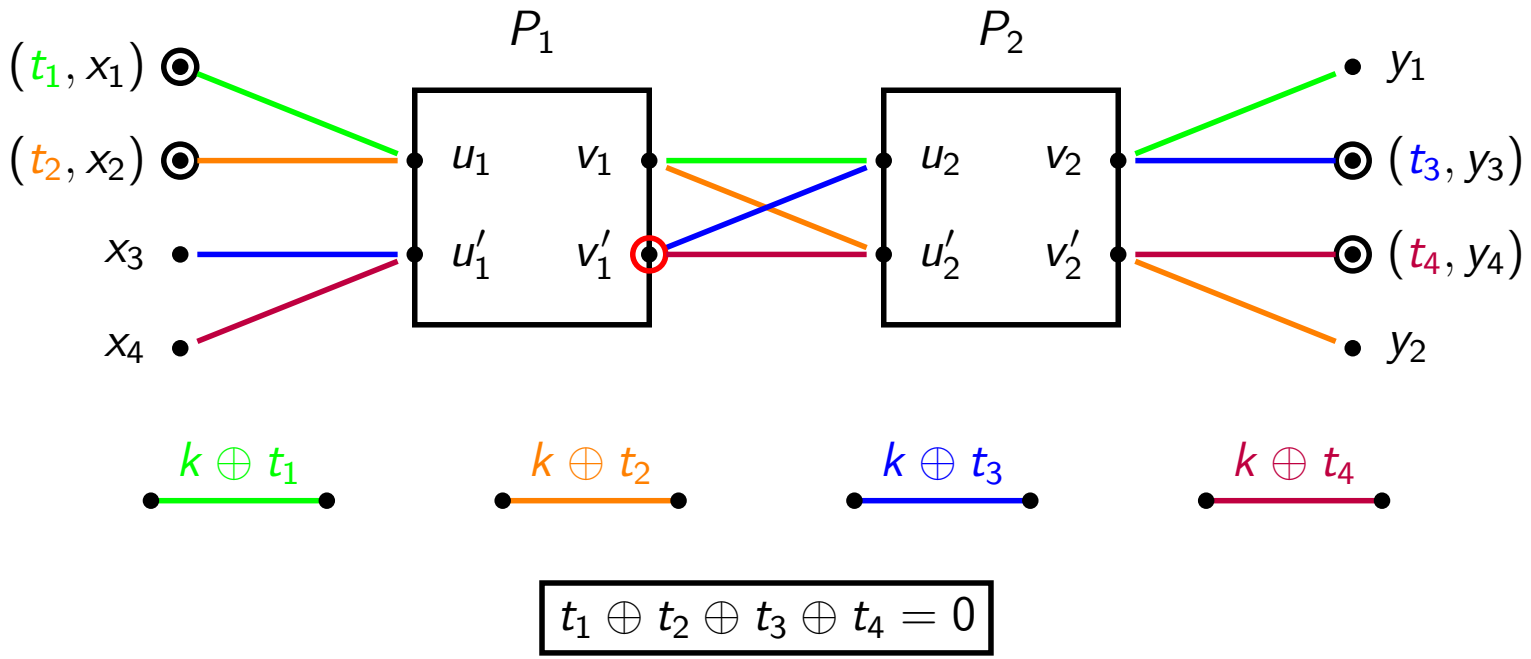


$$t_1 \oplus t_2 \oplus t_3 \oplus t_4 = 0$$

Check that $x_3 \oplus x_4 = t_3 \oplus t_4$ $(*)$

- 4 queries to the enc/dec oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

Second Try: Two Rounds, Linear TKS

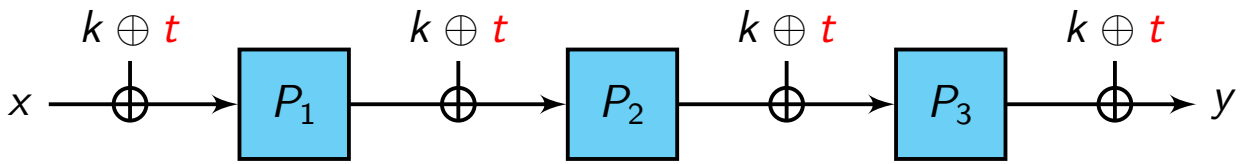


$$t_1 \oplus t_2 \oplus t_3 \oplus t_4 = 0$$

Check that $x_3 \oplus x_4 = t_3 \oplus t_4$ $(*)$

- 4 queries to the enc/dec oracle, 0 queries to P_1, P_2
- $(*)$ holds with proba. 1 for the TEM construction
- $(*)$ holds with proba. 2^{-n} for a random tweakable permutation
- works for any linear TKS

Security for Three Rounds



Theorem ([CS15, FP15])

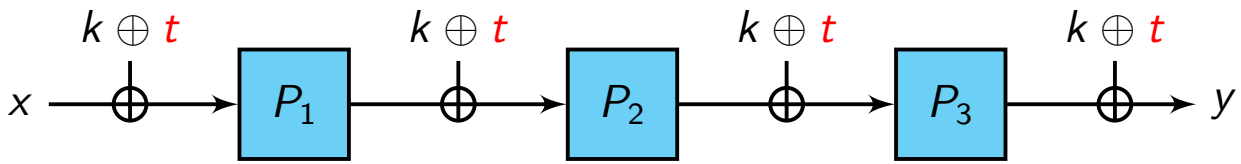
The 3-round TEM with linear TKS is a strong tweakable PRP:

$$\mathbf{Adv}(q_c, q_p) \leq \frac{6q_c q_p}{2^n} + \frac{4q_c^2}{2^n}.$$

Proof sketch:

- adversary can create collisions at input of P_1 or output of 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



Theorem ([CS15, FP15])

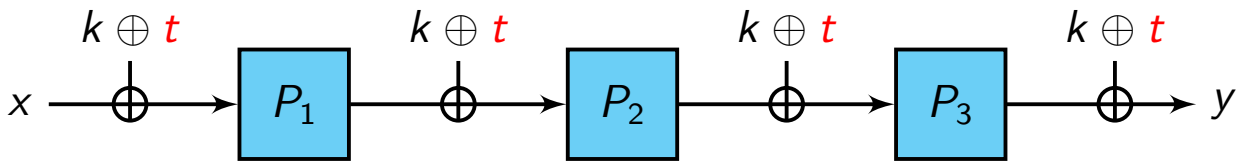
The 3-round TEM with linear TKS is a strong tweakable PRP:

$$\mathbf{Adv}(q_c, q_p) \leq \frac{6q_c q_p}{2^n} + \frac{4q_c^2}{2^n}.$$

Proof sketch:

- adversary can create collisions at input of P_1 or output of 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



Theorem ([CS15, FP15])

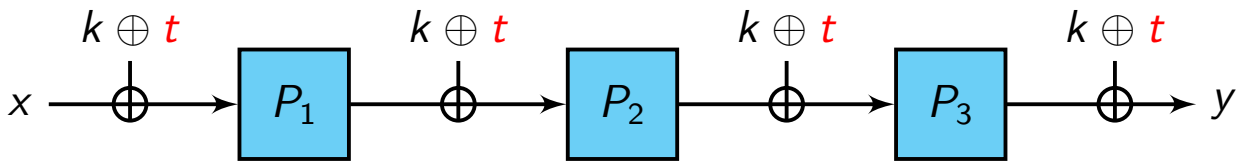
The 3-round TEM with linear TKS is a strong tweakable PRP:

$$\mathbf{Adv}(q_c, q_p) \leq \frac{6q_c q_p}{2^n} + \frac{4q_c^2}{2^n}.$$

Proof sketch:

- adversary can create collisions at input of P_1 or output of 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



Theorem ([CS15, FP15])

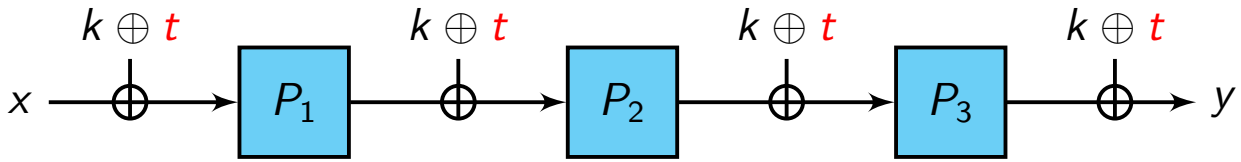
The 3-round TEM with linear TKS is a strong tweakable PRP:

$$\mathbf{Adv}(q_c, q_p) \leq \frac{6q_c q_p}{2^n} + \frac{4q_c^2}{2^n}.$$

Proof sketch:

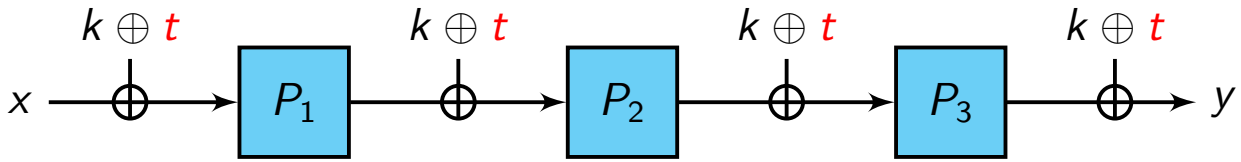
- adversary can create collisions at input of P_1 or output of P_3
- but proba. to create a collision at P_2 is $\lesssim q_c^2/2^n$
- no collision at P_2
  $\Rightarrow \sim$ single-key security of 1-round EM $\lesssim q_c q_p/2^n$

Tightness of the Bound



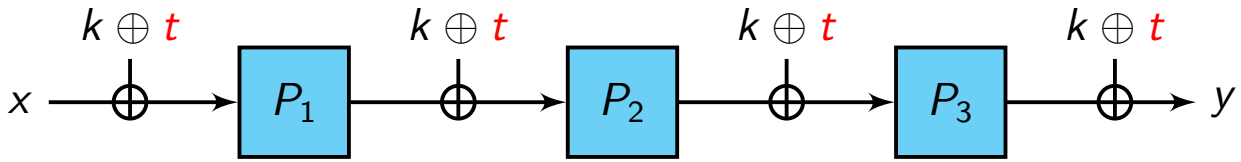
- can be written $\widetilde{E}(k, t, x) = E(k \oplus t, x)$ where E is the conventional 3-round EM cipher with trivial key-schedule
- $\Rightarrow$ secure up to $2^{n/2}$ queries *at best* by a simple collision attack:
  1. query $c_i = \widetilde{E}_{k^*}(t_i, 0) = E(k^* \oplus t_i, 0)$ for $2^{n/2}$ tweaks t_i
  2. compute $c'_j = \widetilde{E}_{k_j}(0, 0) = E(k_j, 0)$ for $2^{n/2}$ keys k_j
  3. look for a collision $c_i = c'_j$
  4. w.h.p., the real key is $k^* = t_i \oplus k_j$
- $\Rightarrow$ increasing the number of rounds does not improve security

Tightness of the Bound



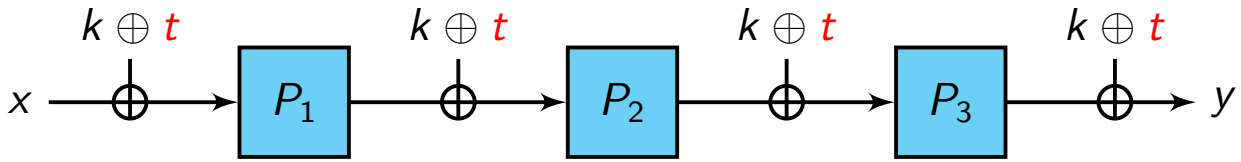
- can be written $\widetilde{E}(k, t, x) = E(k \oplus t, x)$ where E is the conventional 3-round EM cipher with trivial key-schedule
- $\Rightarrow$ secure up to $2^{n/2}$ queries *at best* by a simple collision attack:
  1. query $c_i = \widetilde{E}_{k^*}(t_i, 0) = E(k^* \oplus t_i, 0)$ for $2^{n/2}$ tweaks t_i
  2. compute $c'_j = \widetilde{E}_{k_j}(0, 0) = E(k_j, 0)$ for $2^{n/2}$ keys k_j
  3. look for a collision $c_i = c'_j$
  4. w.h.p., the real key is $k^* = t_i \oplus k_j$
- $\Rightarrow$ increasing the number of rounds does not improve security

Tightness of the Bound



- can be written $\widetilde{E}(k, t, x) = E(k \oplus t, x)$ where E is the conventional 3-round EM cipher with trivial key-schedule
- $\Rightarrow$ secure up to $2^{n/2}$ queries *at best* by a simple collision attack:
  1. query $c_i = \widetilde{E}_{k^*}(t_i, 0) = E(k^* \oplus t_i, 0)$ for $2^{n/2}$ tweaks t_i
  2. compute $c'_j = \widetilde{E}_{k_j}(0, 0) = E(k_j, 0)$ for $2^{n/2}$ keys k_j
  3. look for a collision $c_i = c'_j$
  4. w.h.p., the real key is $k^* = t_i \oplus k_j$
- $\Rightarrow$ increasing the number of rounds does not improve security

Tightness of the Bound



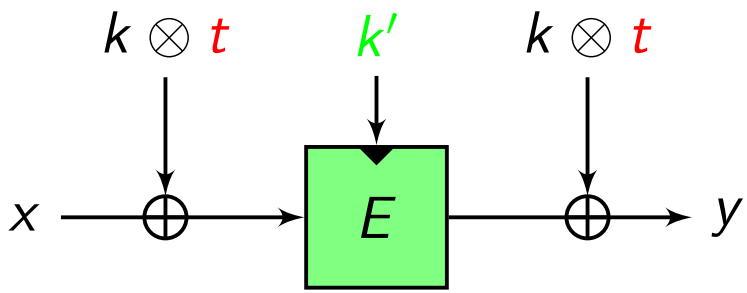
- can be written $\widetilde{E}(k, t, x) = E(k \oplus t, x)$ where E is the conventional 3-round EM cipher with trivial key-schedule
- $\Rightarrow$ secure up to $2^{n/2}$ queries *at best* by a simple collision attack:
  1. query $c_i = \widetilde{E}_{k^*}(t_i, 0) = E(k^* \oplus t_i, 0)$ for $2^{n/2}$ tweaks t_i
  2. compute $c'_j = \widetilde{E}_{k_j}(0, 0) = E(k_j, 0)$ for $2^{n/2}$ keys k_j
  3. look for a collision $c_i = c'_j$
  4. w.h.p., the real key is $k^* = t_i \oplus k_j$
- $\Rightarrow$ increasing the number of rounds does not improve security

Question

Construction with less permutations?

Back to LRW

- instantiate E with the 1-round Even-Mansour construction



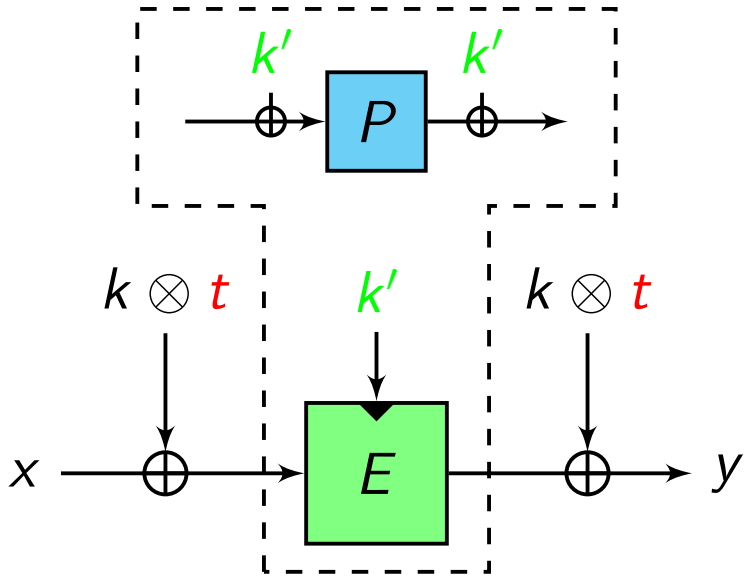
- provably secure in the RPM up to $\sim 2^{n/2}$ queries [FP15, CLS15]:

$$\mathbf{Adv}(q_c, q_p) \leq \frac{q_c^2}{2^n} + \frac{2q_c q_p}{2^n}.$$

- $t \neq 0 \Rightarrow k'$ is superfluous ($k \otimes t$ unif. random for any $t \neq 0$)

Back to LRW

- instantiate E with the 1-round Even-Mansour construction



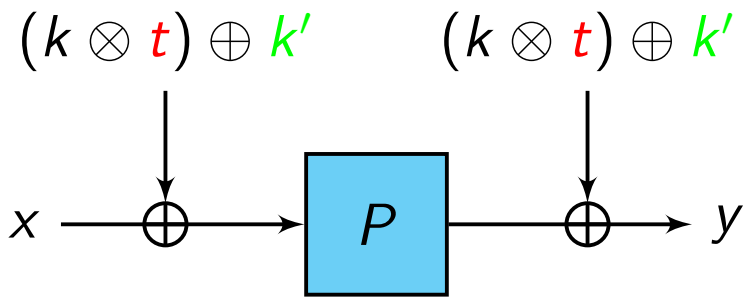
- provably secure in the RPM up to $\sim 2^{n/2}$ queries [FP15, CLS15]:

$$\mathbf{Adv}(q_c, q_p) \leq \frac{q_c^2}{2^n} + \frac{2q_c q_p}{2^n}.$$

- $t \neq 0 \Rightarrow k'$ is superfluous ($k \otimes t$ unif. random for any $t \neq 0$)

Back to LRW

- instantiate E with the 1-round Even-Mansour construction



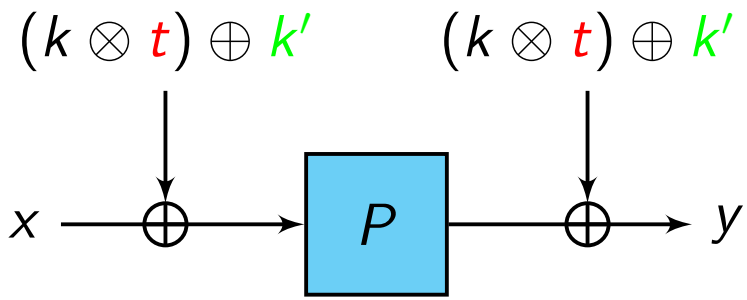
- provably secure in the RPM up to $\sim 2^{n/2}$ queries [FP15, CLS15]:

$$\mathbf{Adv}(q_c, q_p) \leq \frac{q_c^2}{2^n} + \frac{2q_c q_p}{2^n}.$$

- $t \neq 0 \Rightarrow k'$ is superfluous ($k \otimes t$ unif. random for any $t \neq 0$)

Back to LRW

- instantiate E with the 1-round Even-Mansour construction



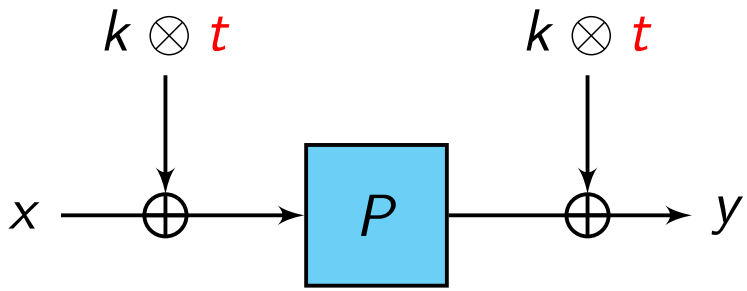
- provably secure in the RPM up to $\sim 2^{n/2}$ queries [FP15, CLS15]:

$$\mathbf{Adv}(q_c, q_p) \leq \frac{q_c^2}{2^n} + \frac{2q_c q_p}{2^n}.$$

- $t \neq 0 \Rightarrow k'$ is superfluous ($k \otimes t$ unif. random for any $t \neq 0$)

Back to LRW

- instantiate E with the 1-round Even-Mansour construction



- provably secure in the RPM up to $\sim 2^{n/2}$ queries [FP15, CLS15]:

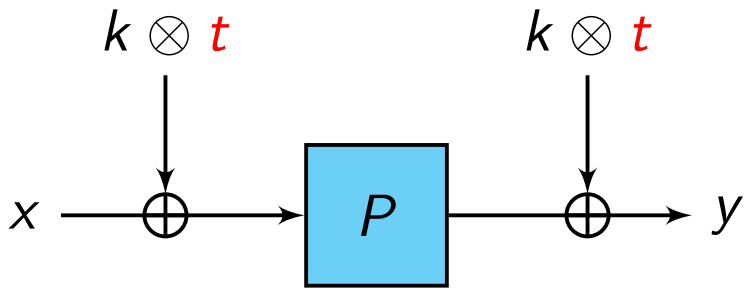
$$\mathbf{Adv}(q_c, q_p) \leq \frac{q_c^2}{2^n} + \frac{2q_c q_p}{2^n}.$$

- $t \neq 0 \Rightarrow k'$ is superfluous ($k \otimes t$ unif. random for any $t \neq 0$)

Back to LRW

- instantiate E with the 1-round Even-Mansour construction

Non-Linear Tweakable Even-Mansour (NL-TEM) construction



- provably secure in the RPM up to $\sim 2^{n/2}$ queries [FP15, CLS15]:

$$\mathbf{Adv}(q_c, q_p) \leq \frac{q_c^2}{2^n} + \frac{2q_c q_p}{2^n}.$$

- $t \neq 0 \Rightarrow k'$ is superfluous ($k \otimes t$ unif. random for any $t \neq 0$)

Birthday-Bound Security: Wrap-up

Two constructions provably secure up to the birthday bound:

1. linear TKS

2. nonlinear TKS

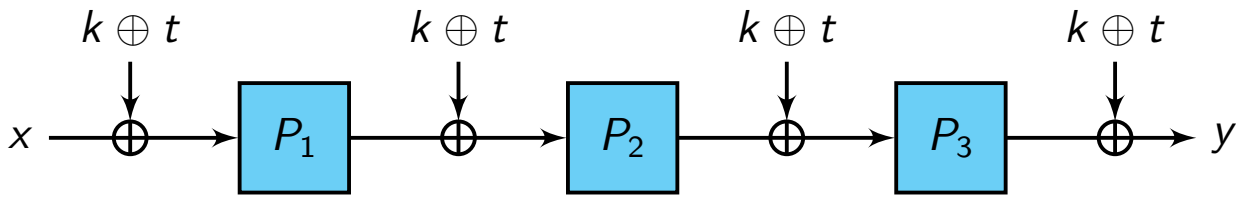
Question

Constructions secure beyond the birthday-bound?

Birthday-Bound Security: Wrap-up

Two constructions provably secure up to the birthday bound:

1. linear TKS



2. nonlinear TKS

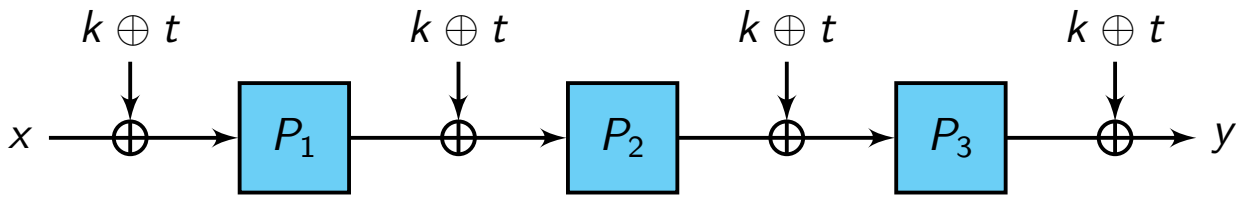
Question

Constructions secure beyond the birthday-bound?

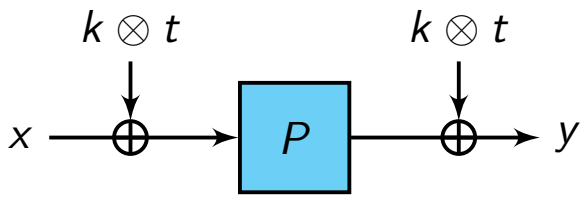
Birthday-Bound Security: Wrap-up

Two constructions provably secure up to the birthday bound:

1. linear TKS



2. nonlinear TKS



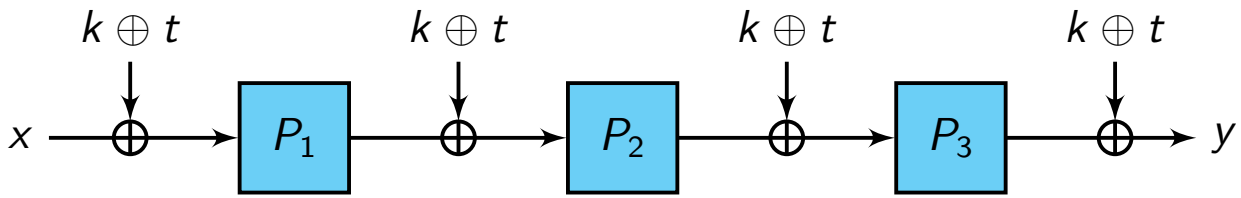
Question

Constructions secure beyond the birthday-bound?

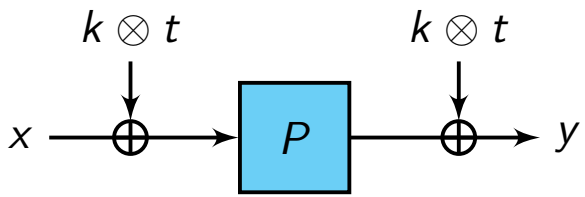
Birthday-Bound Security: Wrap-up

Two constructions provably secure up to the birthday bound:

1. linear TKS



2. nonlinear TKS

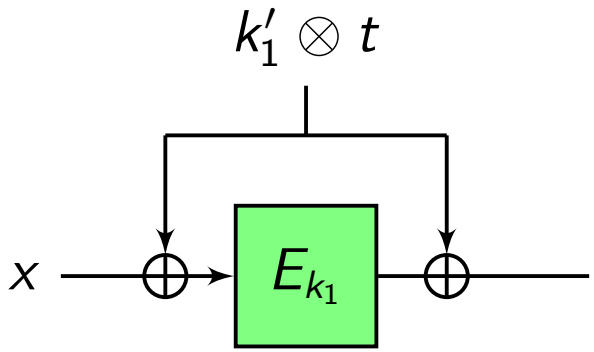


Question

Constructions secure beyond the birthday-bound?

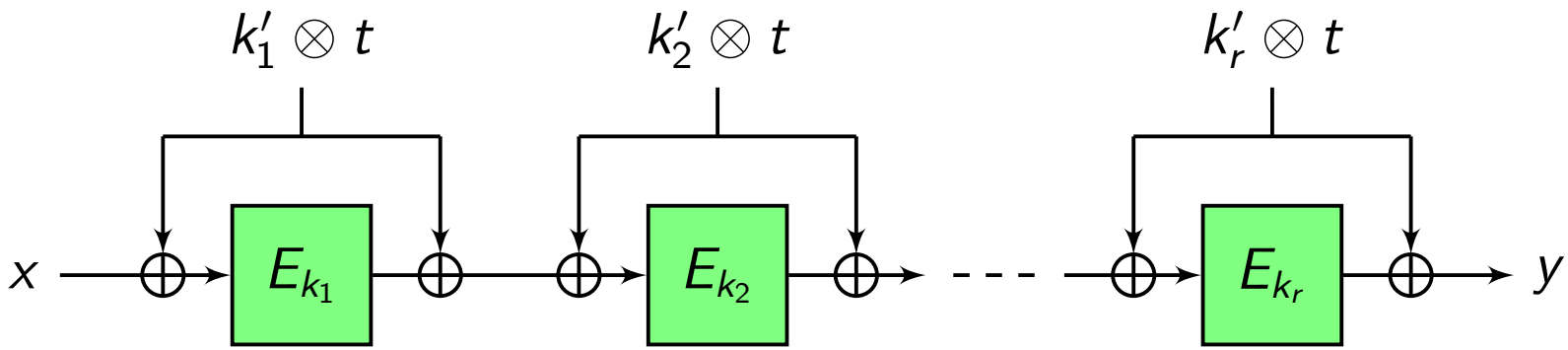
Outline

Cascading the LRW Construction



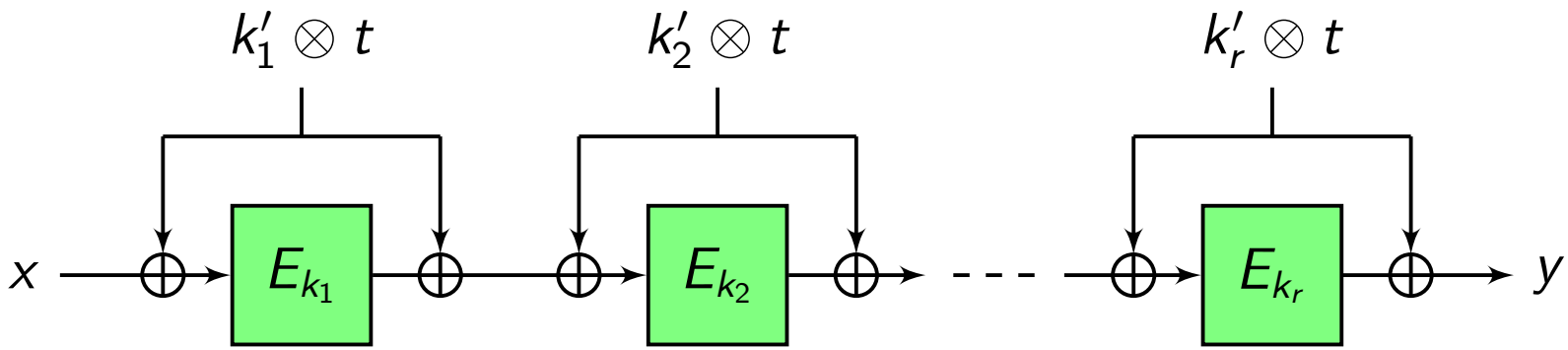
- $k_1, \ldots, k_r$ and $k_1', \ldots, k_r'$ independent keys
  $\Rightarrow$ total key-length $= r(\kappa + n)$
- 2 rounds: provably secure up to $\sim 2^{2n/3}$ queries [LST12]
- r rounds, r even: provably secure up to $\sim 2^{\frac{rn}{r+2}}$ queries [LS13]
- NB: only assuming E is a PRP
  (standard security notion, no ideal model)

Cascading the LRW Construction



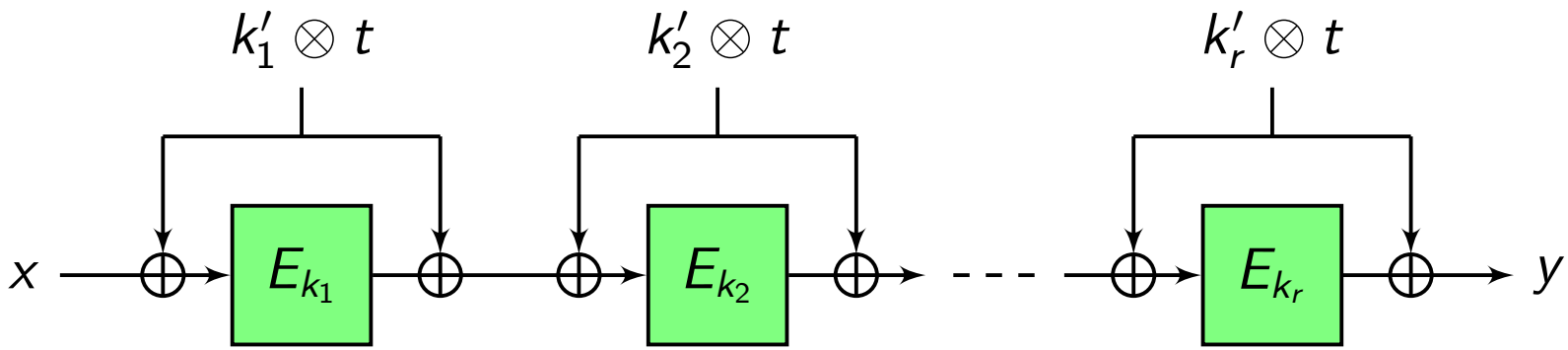
- $k_1, \ldots, k_r$ and $k'_1, \ldots, k'_r$ independent keys
  $\Rightarrow$ total key-length $= r(\kappa + n)$
- 2 rounds: provably secure up to $\sim 2^{2n/3}$ queries [LST12]
- r rounds, r even: provably secure up to $\sim 2^{\frac{rn}{r+2}}$ queries [LS13]
- NB: only assuming E is a PRP
  (standard security notion, no ideal model)

Cascading the LRW Construction



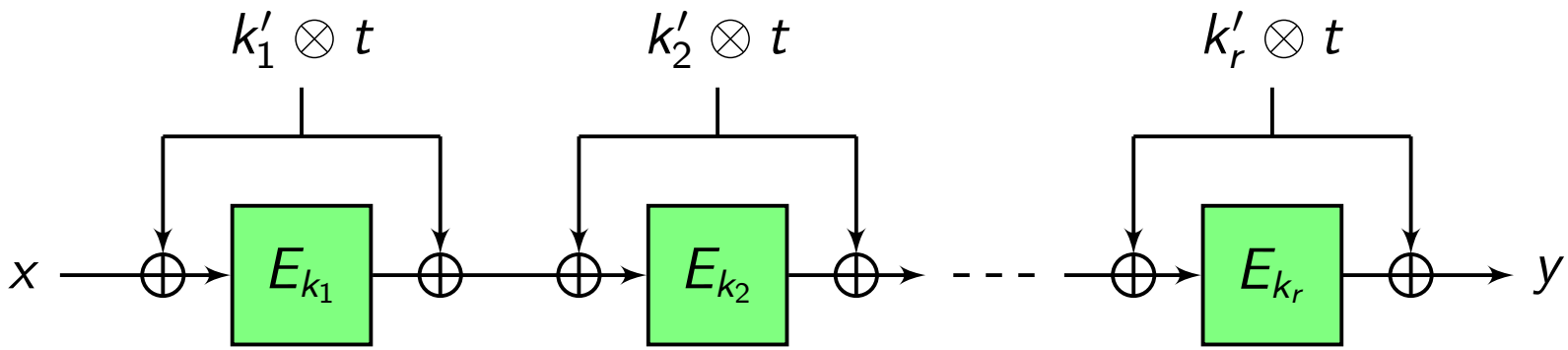
- $k_1, \ldots, k_r$ and $k'_1, \ldots, k'_r$ independent keys
  $\Rightarrow$ total key-length $= r(\kappa + n)$
- 2 rounds: provably secure up to $\sim 2^{2n/3}$ queries [LST12]
- r rounds, r even: provably secure up to $\sim 2^{\frac{rn}{r+2}}$ queries [LS13]
- NB: only assuming E is a PRP
  (standard security notion, no ideal model)

Cascading the LRW Construction



- $k_1, \ldots, k_r$ and $k'_1, \ldots, k'_r$ independent keys
  $\Rightarrow$ total key-length $= r(\kappa + n)$
- 2 rounds: provably secure up to $\sim 2^{2n/3}$ queries [LST12]
- r rounds, r even: provably secure up to $\sim 2^{\frac{rn}{r+2}}$ queries [LS13]
- NB: only assuming E is a PRP
  (standard security notion, no ideal model)

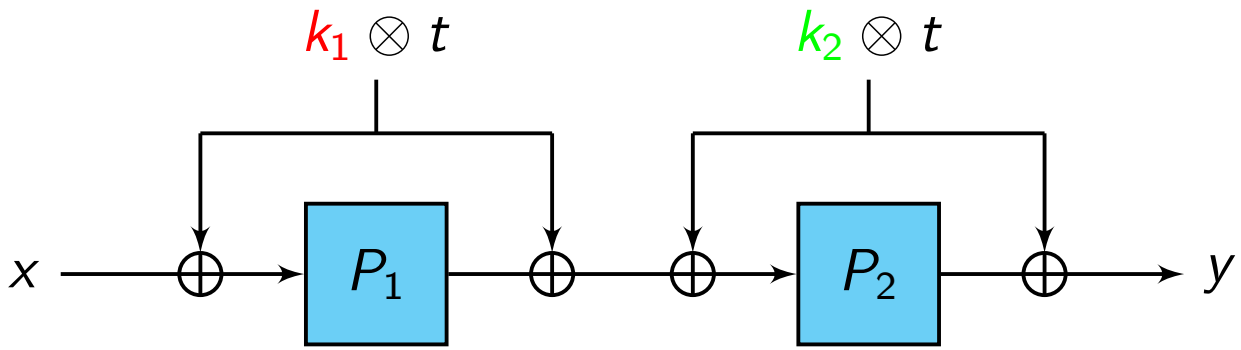
Cascading the LRW Construction



- $k_1, \ldots, k_r$ and $k'_1, \ldots, k'_r$ independent keys
  $\Rightarrow$ total key-length $= r(\kappa + n)$
- 2 rounds: provably secure up to $\sim 2^{2n/3}$ queries [LST12]
- r rounds, r even: provably secure up to $\sim 2^{\frac{rn}{r+2}}$ queries [LS13]
- NB: only assuming E is a PRP
  (standard security notion, no ideal model)

Cascading the NL-TEM Construction

- k_1, k_2 independent n-bit keys



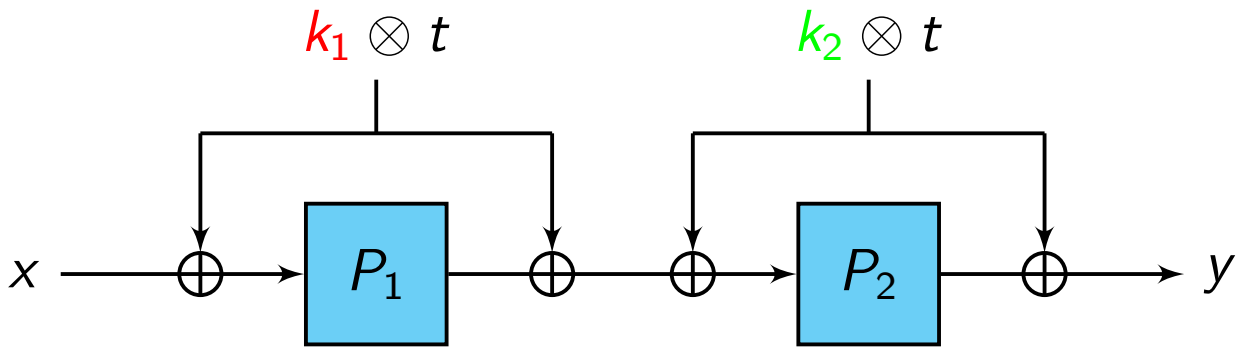
Theorem ([CLS15])

The 2-round NL-TEM construction is secure up to $\sim 2^{2n/3}$ queries in the RPM:

$$\mathbf{Adv}(q_c, q_p) \leq \frac{34 q_c^{3/2}}{2^n} + \frac{30\sqrt{q_c} q_p}{2^n}.$$

Cascading the NL-TEM Construction

- k_1, k_2 independent n-bit keys

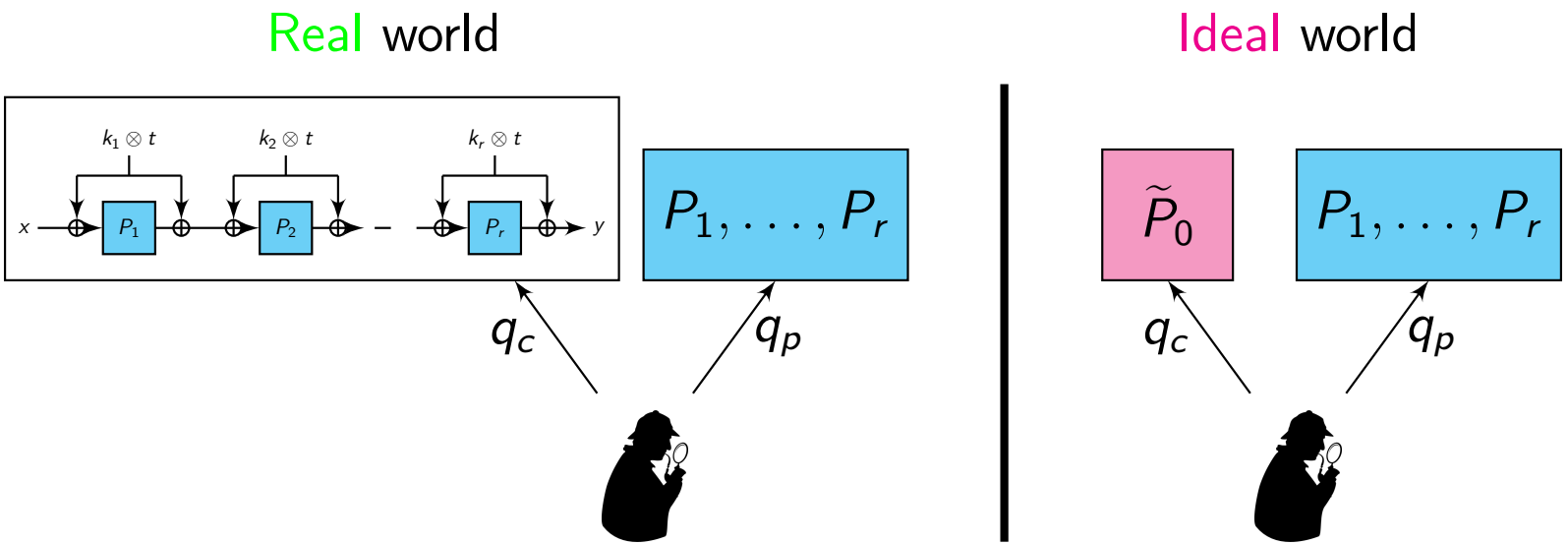


Theorem ([CLS15])

The 2-round NL-TEM construction is secure up to $\sim 2^{2n/3}$ *queries in the RPM:*

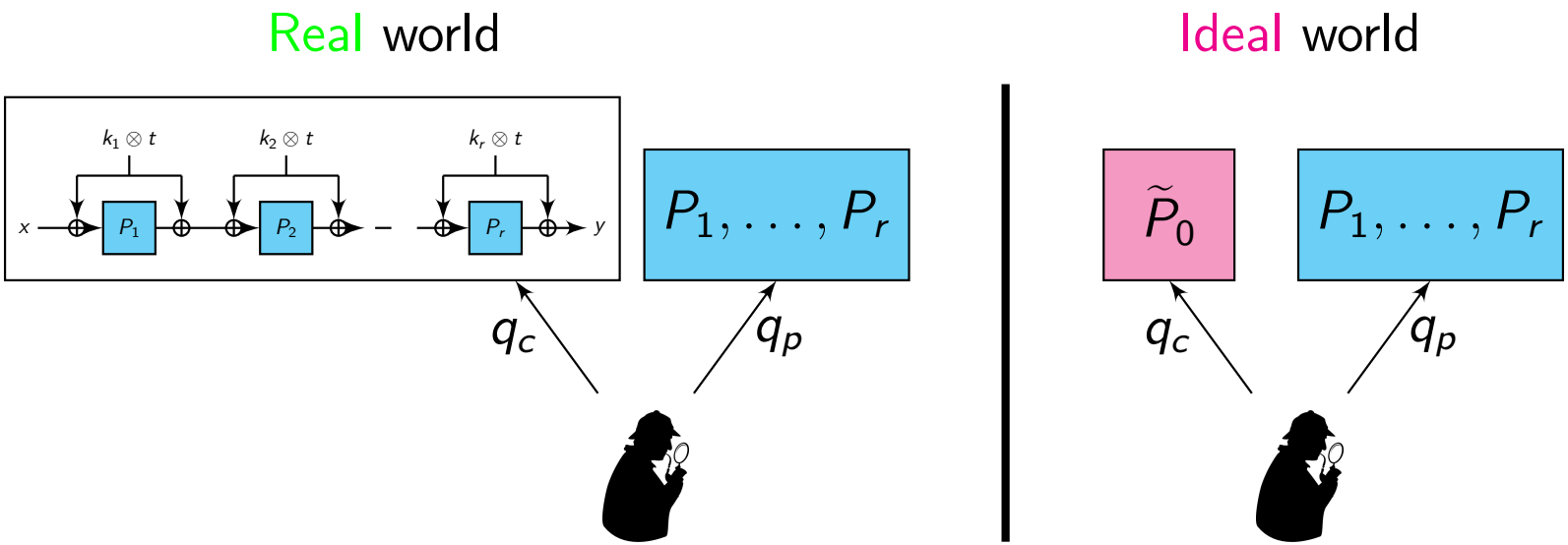
$$\mathbf{Adv}(q_c, q_p) \leq \frac{34 q_c^{3/2}}{2^n} + \frac{30\sqrt{q_c} q_p}{2^n}.$$

Proof Technique: H-coefficients



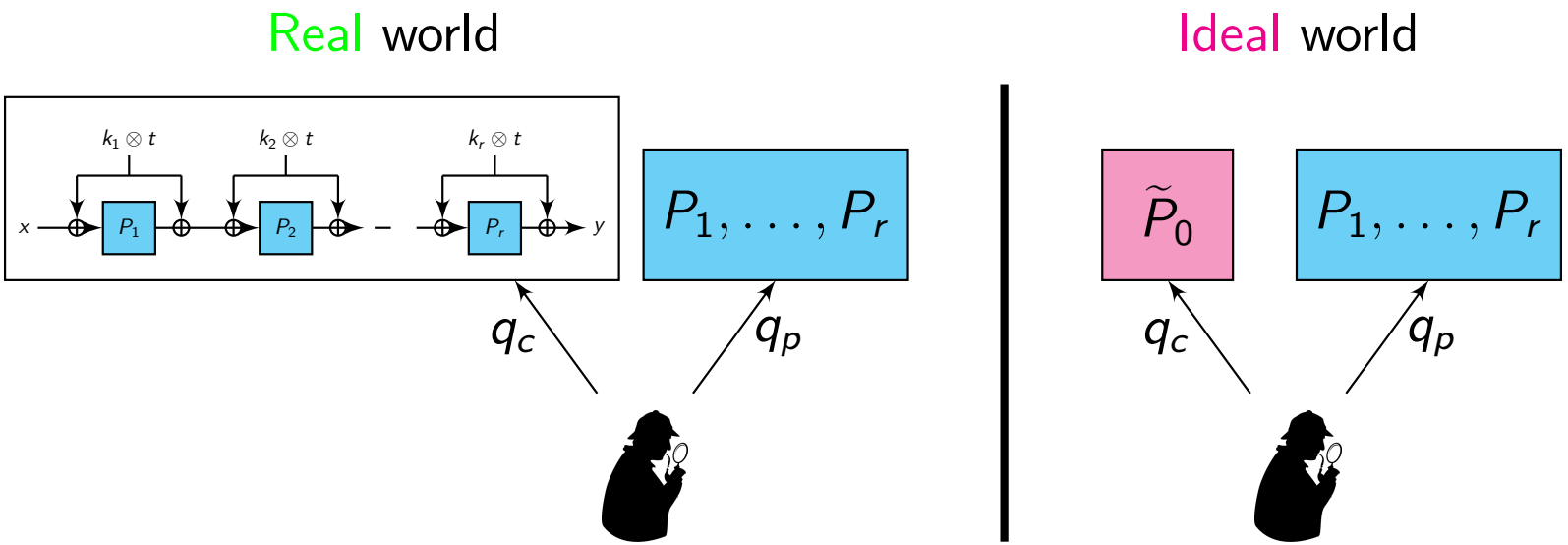
1. consider the transcript of all queries of $\mathcal{D}$ to the construction and to the inner permutations
2. define bad transcripts and show that their probability is small (in the ideal world)
3. show that good transcripts are almost as probable in the real and the ideal world

Proof Technique: H-coefficients



1. consider the transcript of all queries of $\mathcal{D}$ to the construction and to the inner permutations
2. define bad transcripts and show that their probability is small (in the ideal world)
3. show that good transcripts are almost as probable in the real and the ideal world

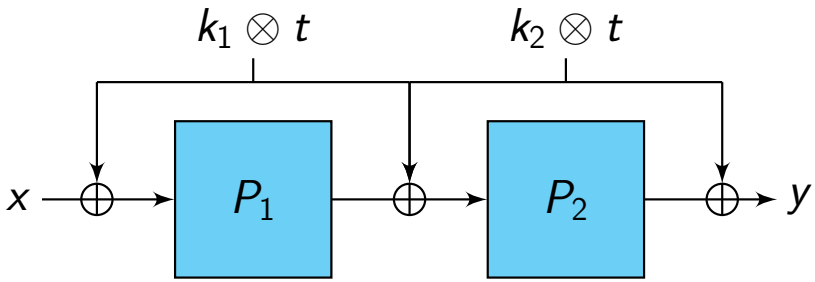
Proof Technique: H-coefficients



1. consider the transcript of all queries of $\mathcal{D}$ to the construction and to the inner permutations
2. define bad transcripts and show that their probability is small (in the ideal world)
3. show that good transcripts are almost as probable in the real and the ideal world

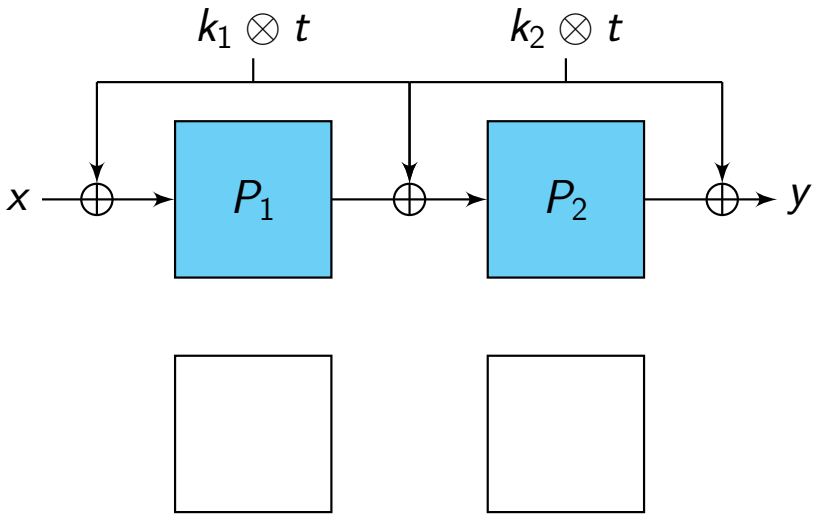
Bad Transcripts

- one needs to avoid "two-fold" collisions:



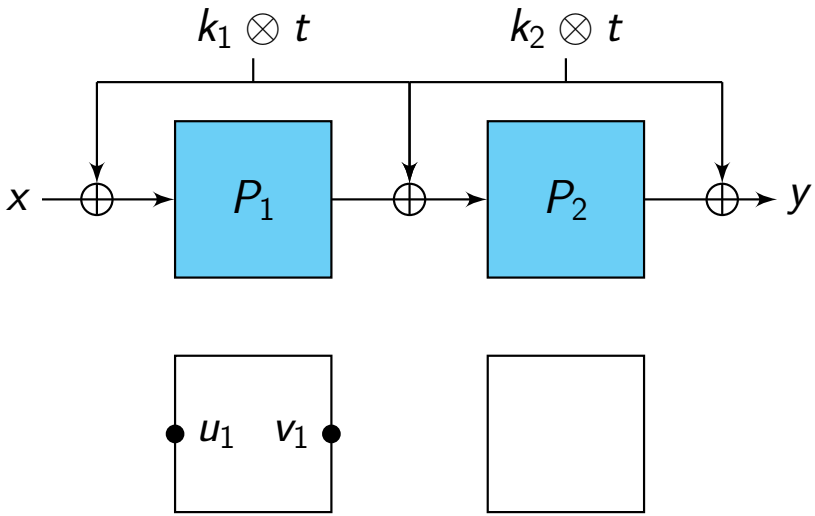
Bad Transcripts

- one needs to avoid "two-fold" collisions:



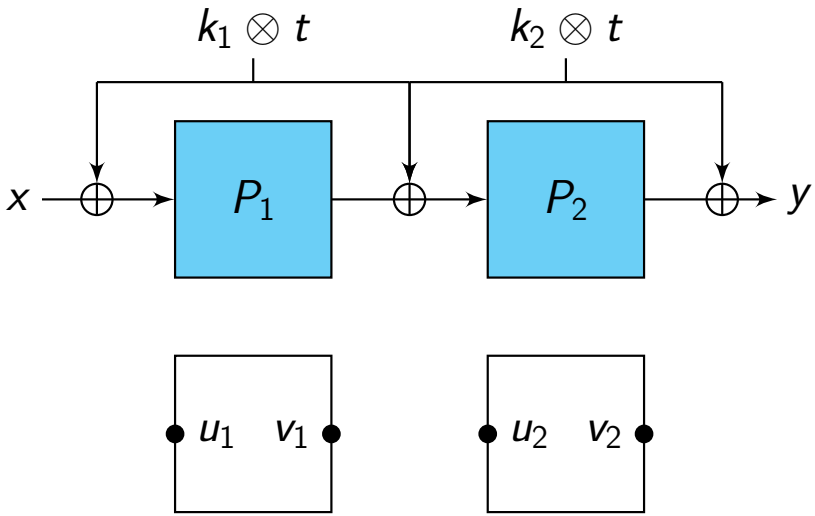
Bad Transcripts

- one needs to avoid "two-fold" collisions:



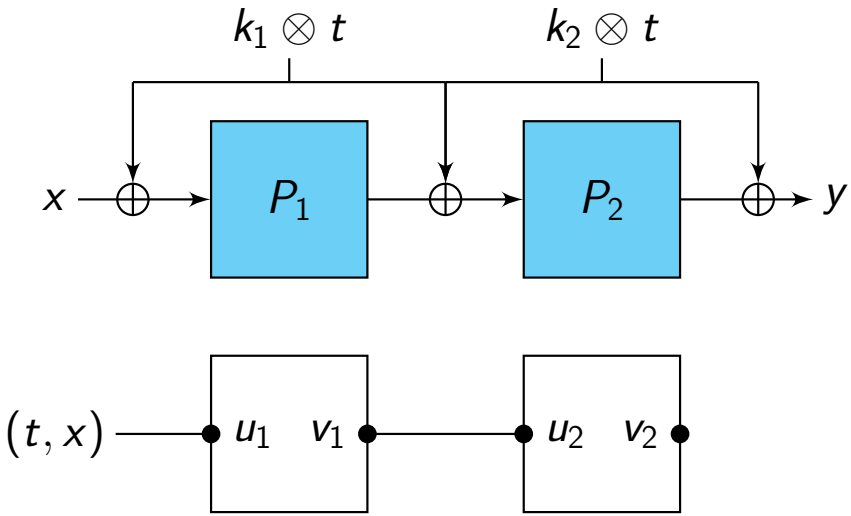
Bad Transcripts

- one needs to avoid "two-fold" collisions:



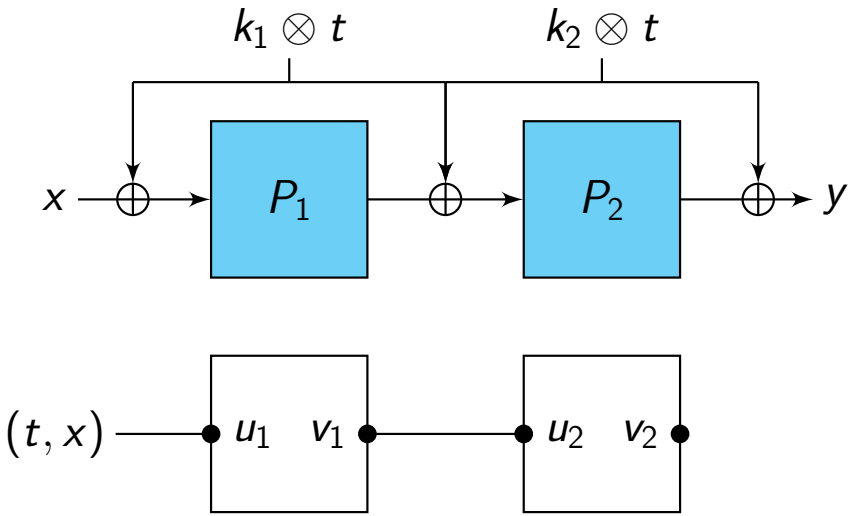
Bad Transcripts

- one needs to avoid "two-fold" collisions:



Bad Transcripts

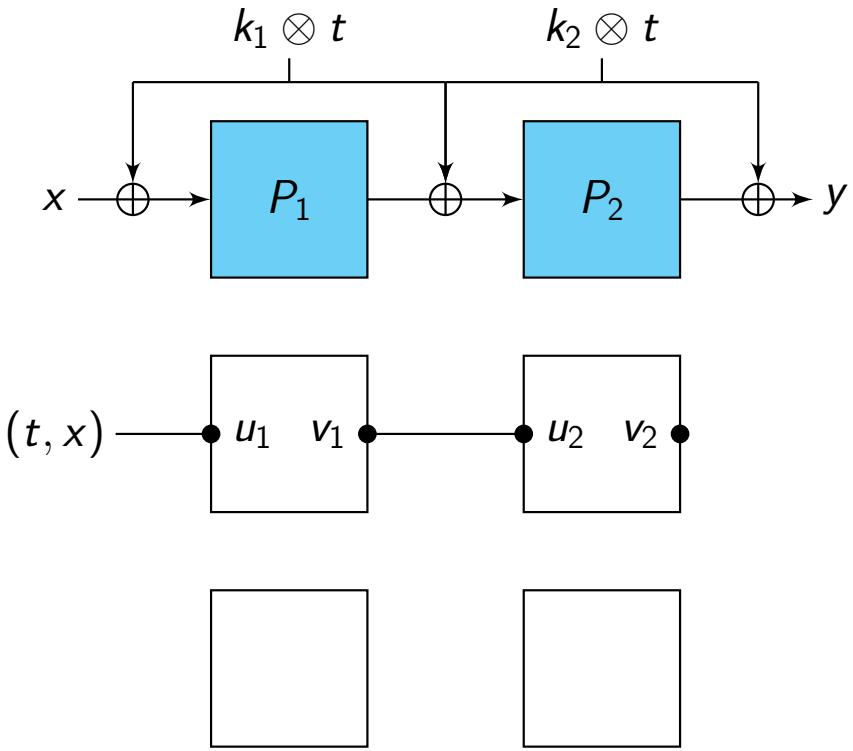
- one needs to avoid "two-fold" collisions:



$$\text{proba} \leq \frac{q_c q_p^2}{2^{2n}}$$

Bad Transcripts

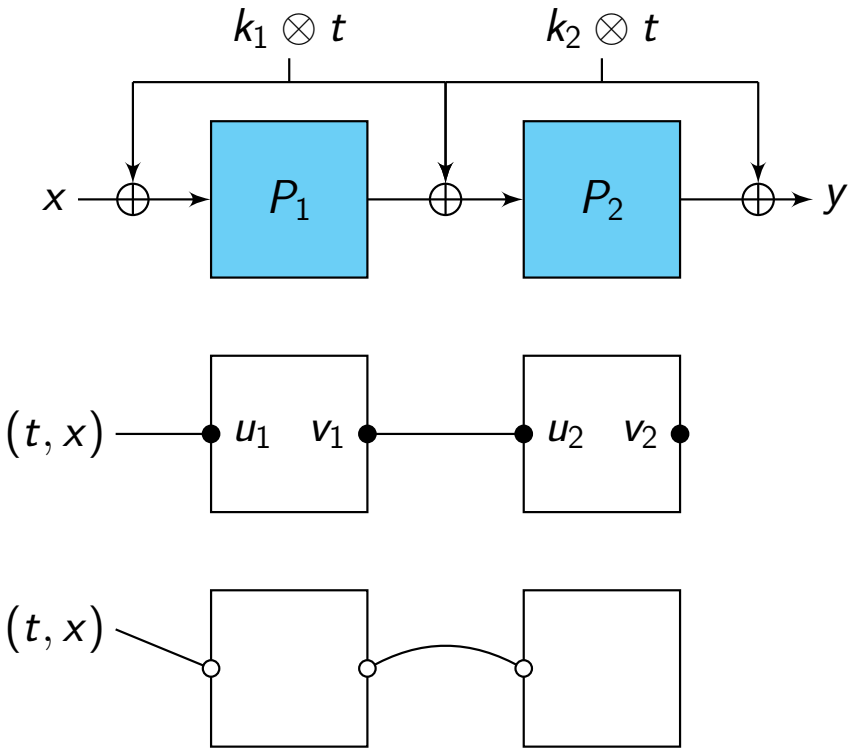
- one needs to avoid "two-fold" collisions:



$$\text{proba} \leq \frac{q_c q_p^2}{2^{2n}}$$

Bad Transcripts

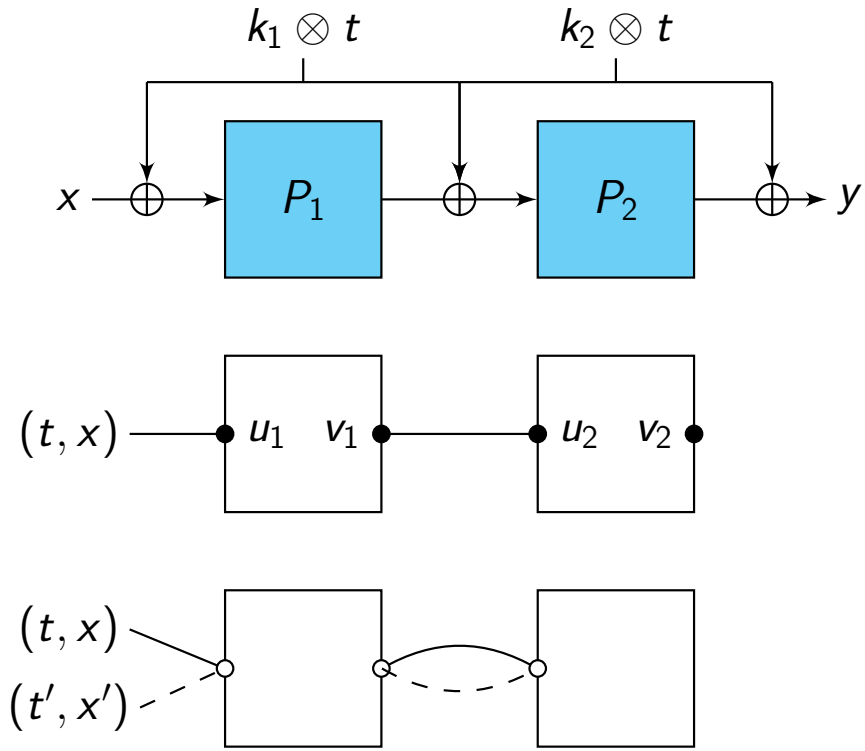
- one needs to avoid "two-fold" collisions:



$$\text{proba} \leq \frac{q_c q_p^2}{2^{2n}}$$

Bad Transcripts

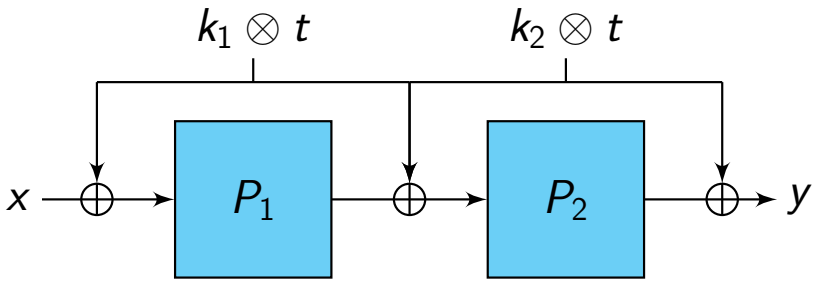
- one needs to avoid "two-fold" collisions:

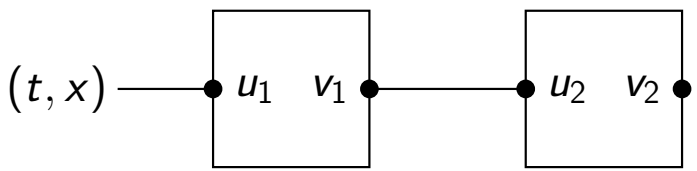


$$\text{proba} \leq \frac{q_c q_p^2}{2^{2n}}$$

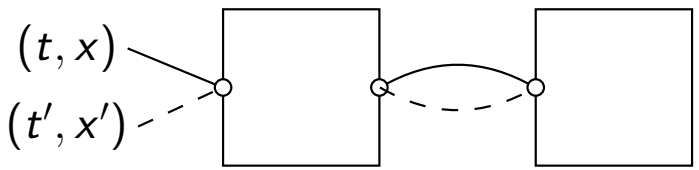
Bad Transcripts

- one needs to avoid "two-fold" collisions:



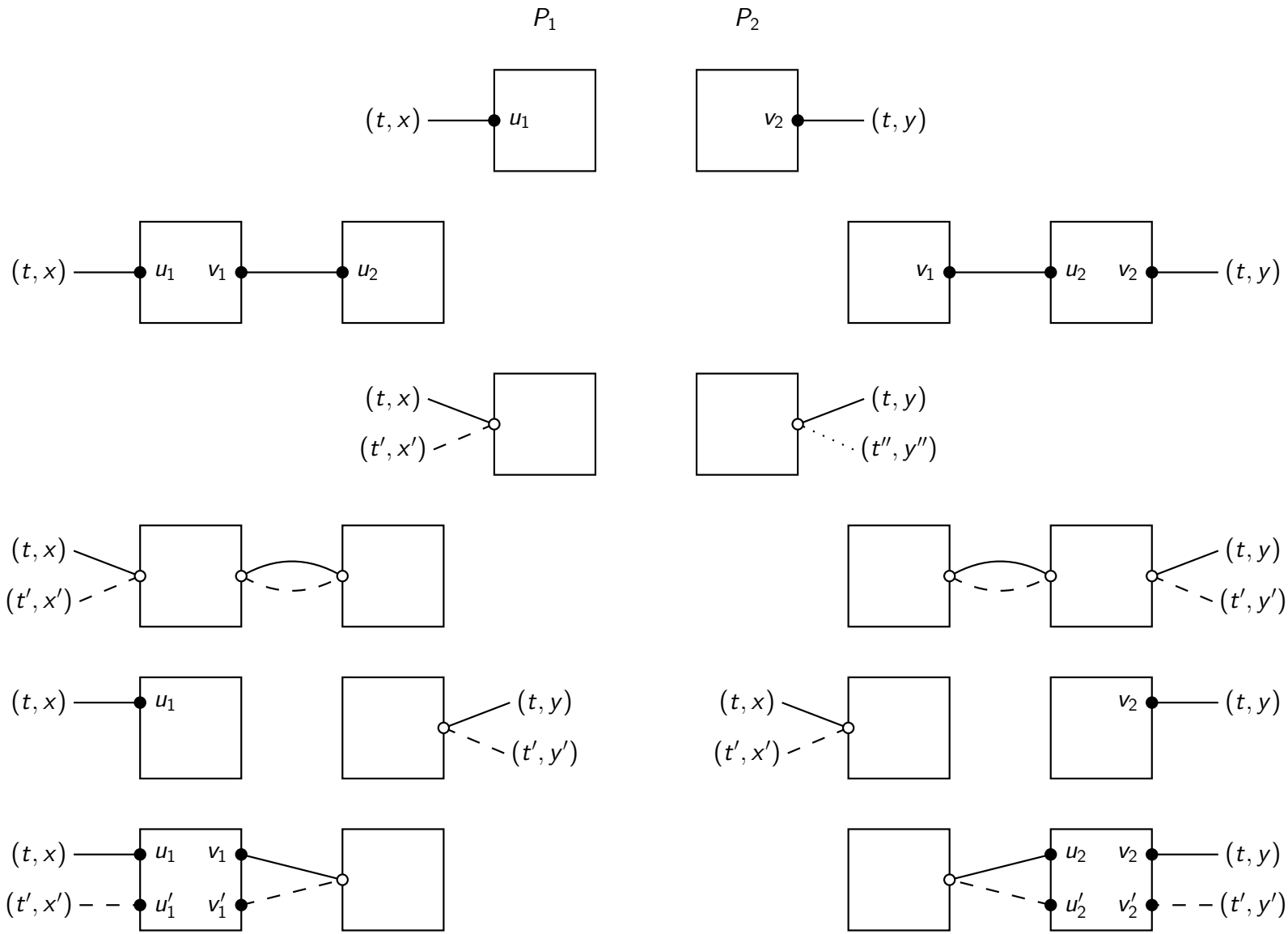


$$\text{proba} \leq \frac{q_c q_p^2}{2^{2n}}$$

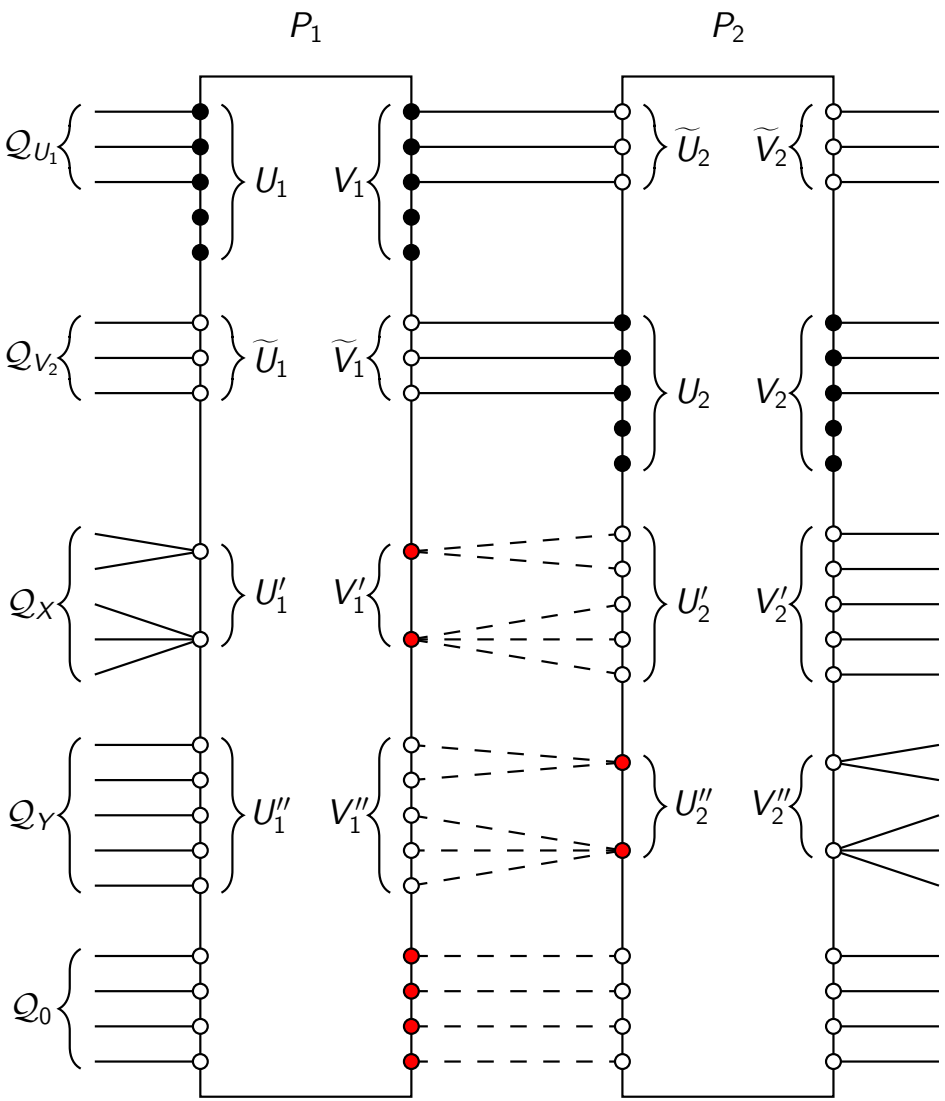


$$\text{proba} \leq \frac{q_c^2}{2^{2n}}$$

The Ten "Bad Collision" Cases

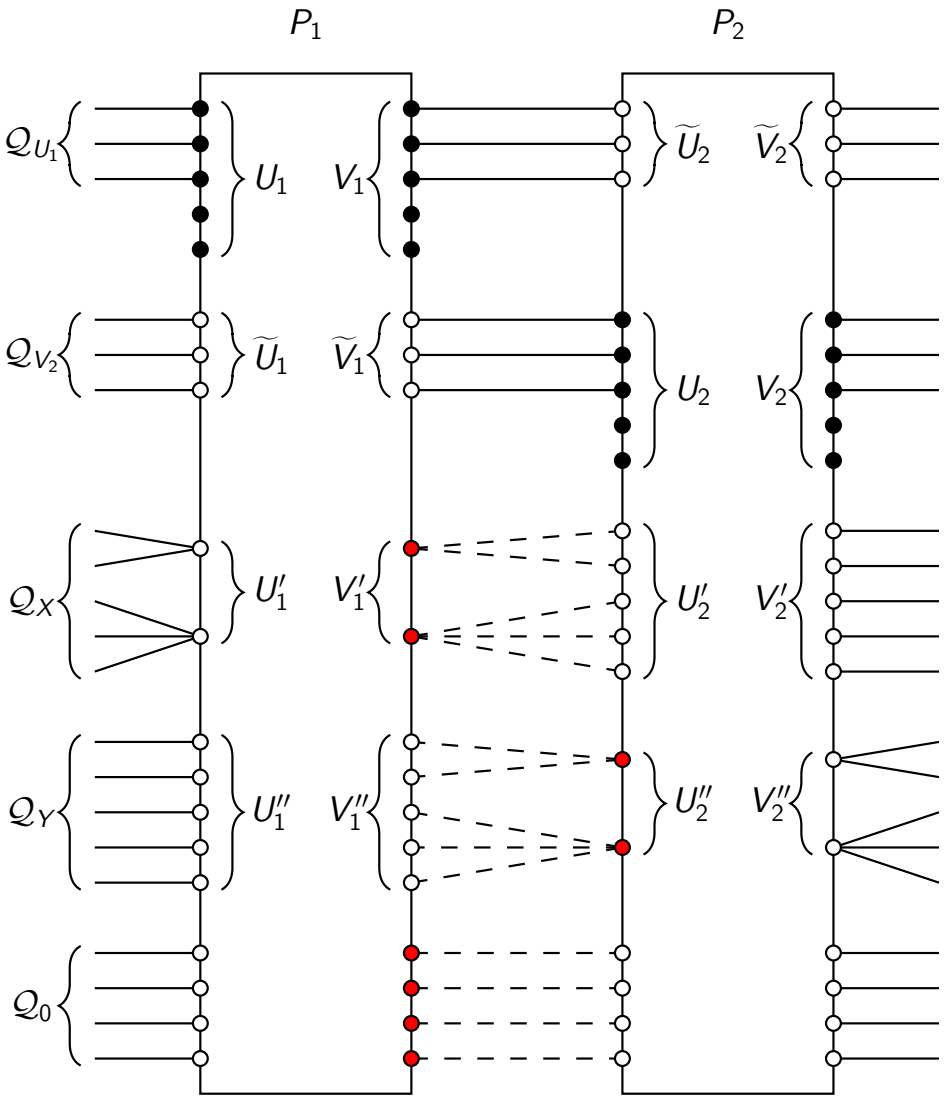


Distribution of Good Transcripts



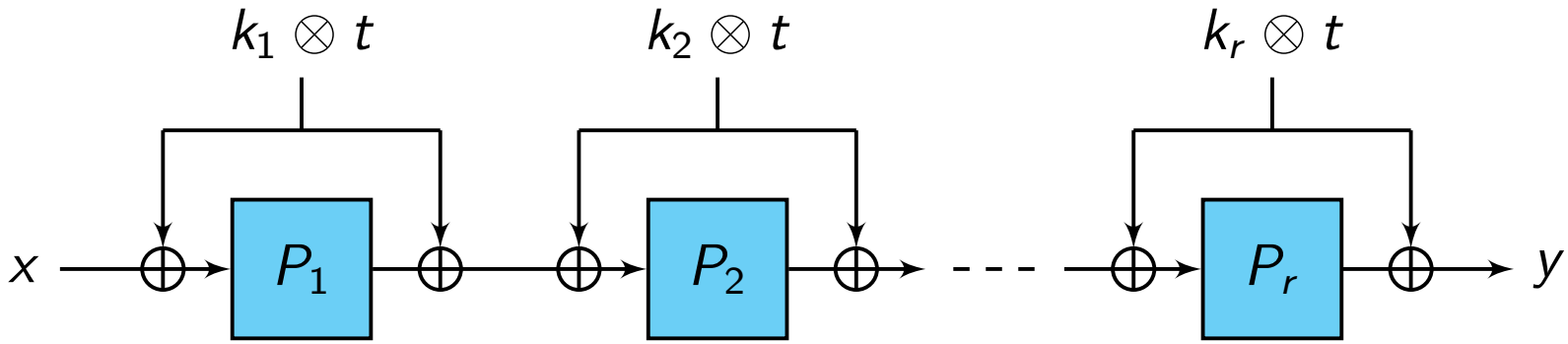
- assuming there are no bad collisions, show that the answers of the TEM construction are close to answers of a random tweakable permutation
- for each query, there is a "fresh" value of P_1 or P_2 which randomizes the output

Distribution of Good Transcripts



- assuming there are no bad collisions, show that the answers of the TEM construction are close to answers of a random tweakable permutation
- for each query, there is a "fresh" value of P_1 or P_2 which randomizes the output

Longer Cascades of the NL-TEM Construction

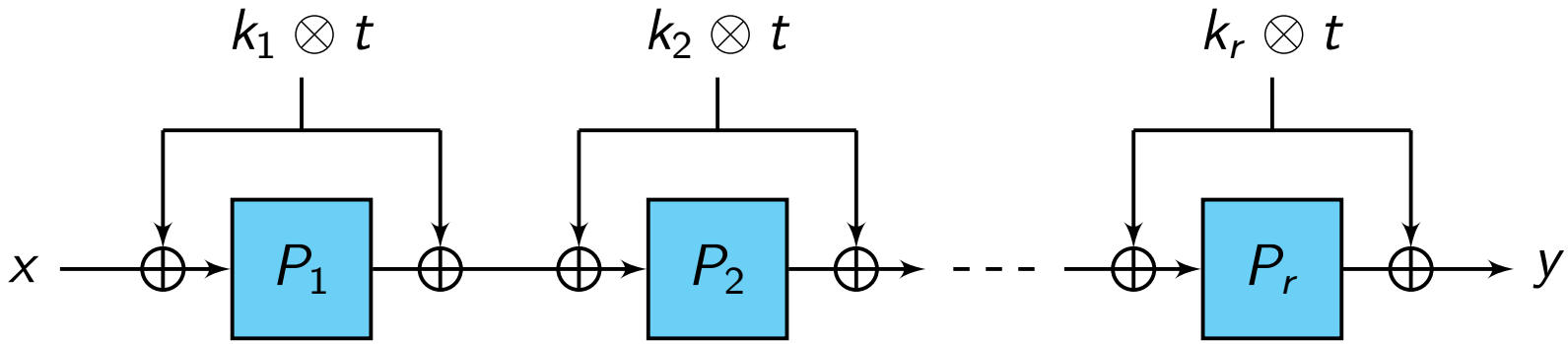


- r rounds, r even, with independent keys $k_1, \ldots, k_r$ secure up to

$$\sim 2^{\frac{rn}{r+2}} = 2^{\frac{(r/2)n}{(r/2)+1}} \text{ queries}$$

- proof:
  1. non-adaptive security for $r/2$ rounds (coupling technique)
  2. adaptive security for r rounds ("two weak make one strong" composition theorem)
- conjecture: secure up to $\sim 2^{\frac{rn}{r+1}}$ queries

Longer Cascades of the NL-TEM Construction

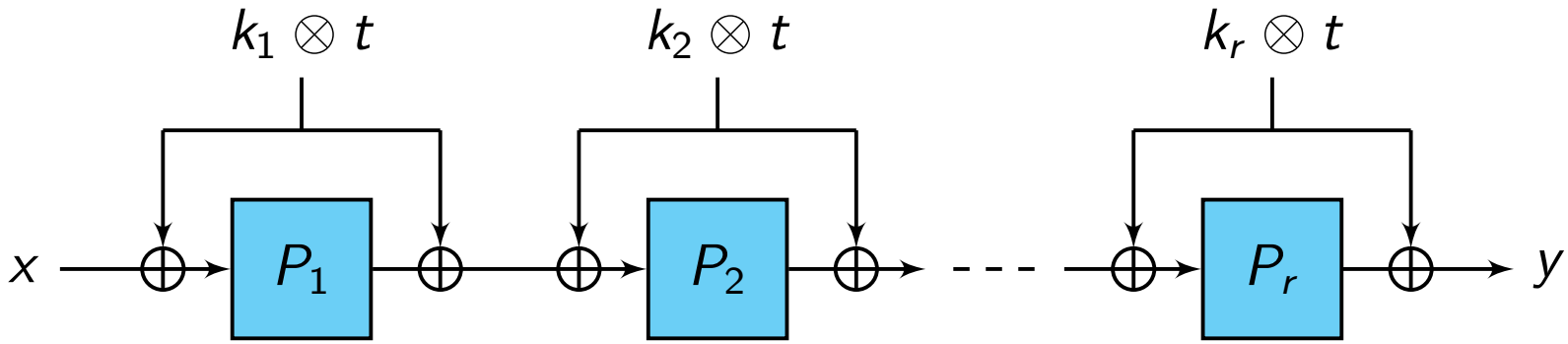


- r rounds, r even, with independent keys $k_1, \ldots, k_r$ secure up to

$$\sim 2^{\frac{rn}{r+2}} = 2^{\frac{(r/2)n}{(r/2)+1}} \text{ queries}$$

- proof:
  1. non-adaptive security for $r/2$ rounds (coupling technique)
  2. adaptive security for r rounds ("two weak make one strong" composition theorem)
- conjecture: secure up to $\sim 2^{\frac{rn}{r+1}}$ queries

Longer Cascades of the NL-TEM Construction

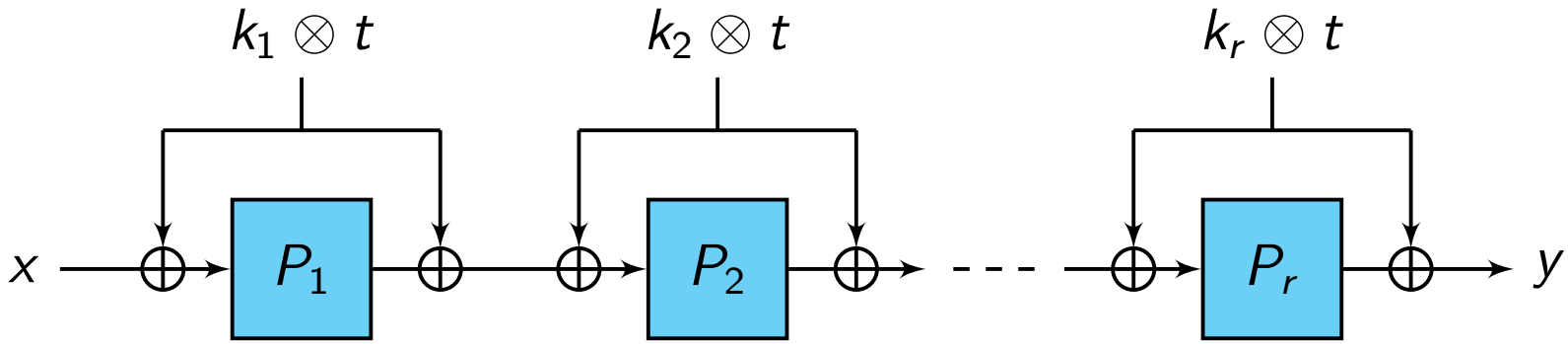


- r rounds, r even, with independent keys $k_1, \ldots, k_r$ secure up to

$$\sim 2^{\frac{rn}{r+2}} = 2^{\frac{(r/2)n}{(r/2)+1}} \text{ queries}$$

- proof:
  1. non-adaptive security for $r/2$ rounds (coupling technique)
  2. adaptive security for r rounds ("two weak make one strong" composition theorem)
- conjecture: secure up to $\sim 2^{\frac{rn}{r+1}}$ queries

Longer Cascades of the NL-TEM Construction



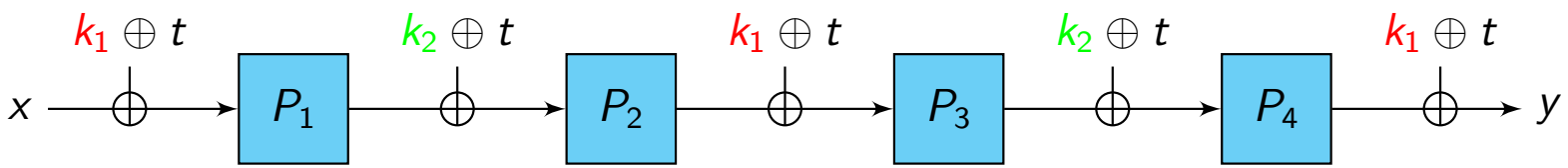
- r rounds, r even, with independent keys $k_1, \ldots, k_r$ secure up to

$$\sim 2^{\frac{rn}{r+2}} = 2^{\frac{(r/2)n}{(r/2)+1}} \text{ queries}$$

- proof:
  1. non-adaptive security for $r/2$ rounds (coupling technique)
  2. adaptive security for r rounds ("two weak make one strong" composition theorem)
- conjecture: secure up to $\sim 2^{\frac{rn}{r+1}}$ queries

BBB Security with a Linear TKS

- k_1, k_2 independent n-bit keys



Theorem (B. Cogliati, Y.S., AC 2015)

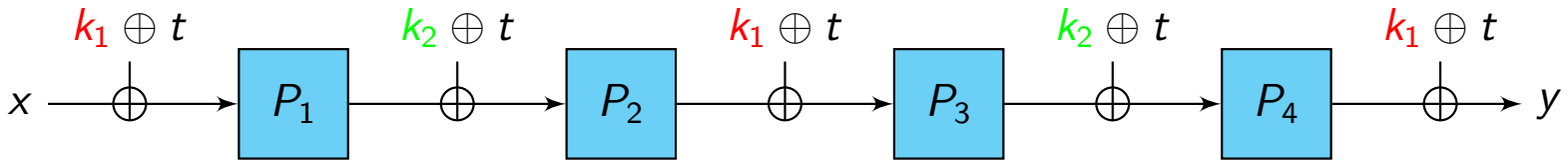
The 4-round TEM with "alternating" linear TKS is secure up to $\sim 2^{2n/3}$ queries in the RPM.

Proof idea:

- exclude bad events related to P_1 and P_4
- "reduction" to 2-round NL-TEM security based on (P_2, P_3)

BBB Security with a Linear TKS

- k_1, k_2 independent n-bit keys



Theorem (B. Cogliati, Y.S., AC 2015)

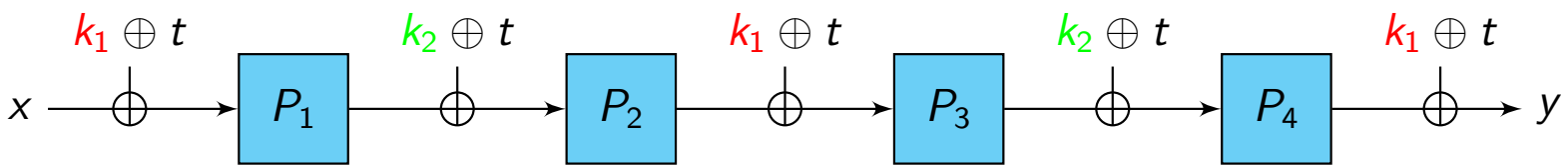
The 4-round TEM with "alternating" linear TKS is secure up to $\sim 2^{2n/3}$ *queries in the RPM.*

Proof idea:

- exclude bad events related to P_1 and P_4
- "reduction" to 2-round NL-TEM security based on (P_2, P_3)

BBB Security with a Linear TKS

- k_1, k_2 independent n-bit keys



Theorem (B. Cogliati, Y.S., AC 2015)

The 4-round TEM with "alternating" linear TKS is secure up to $\sim 2^{2n/3}$ *queries in the RPM.*

Proof idea:

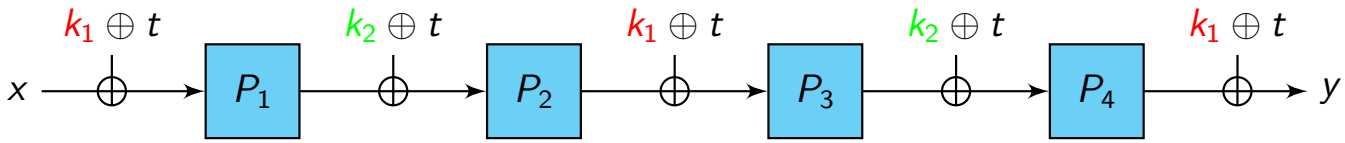
- exclude bad events related to P_1 and P_4
- "reduction" to 2-round NL-TEM security based on (P_2, P_3)

Outline

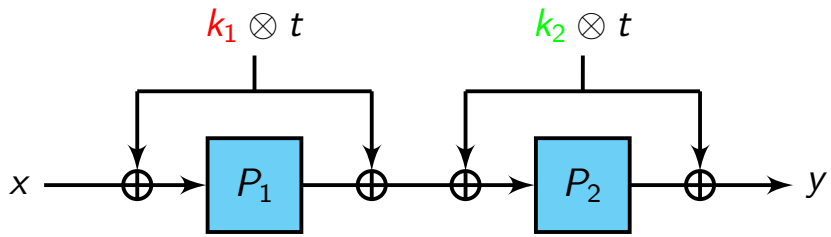
Conclusion

$2^{2n/3}$-secure constructions:

1. linear TKS



2. nonlinear TKS



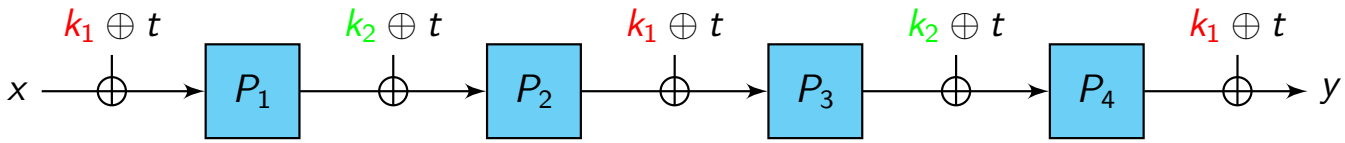
Open problems:

1. prove tight $2^{\frac{rn}{r+1}}$-security for r-round NL-TEM, $r \geq 3$
2. propose a construction with linear TKS and security $> 2^{2n/3}$
3. reduce key length for BBB-security

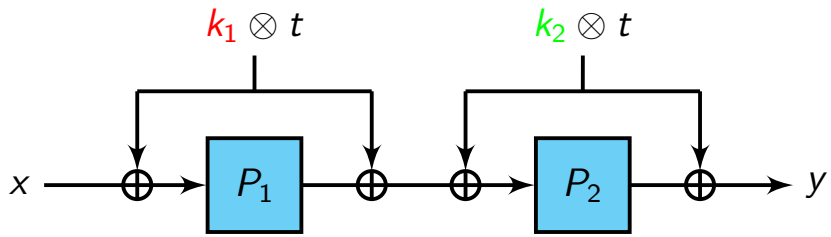
Conclusion

$2^{2n/3}$-secure constructions:

1. linear TKS



2. nonlinear TKS



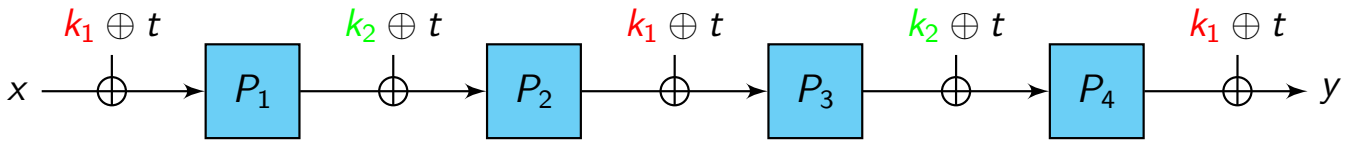
Open problems:

1. prove tight $2^{\frac{rn}{r+1}}$-security for r-round NL-TEM, $r \geq 3$
2. propose a construction with linear TKS and security $> 2^{2n/3}$
3. reduce key length for BBB-security

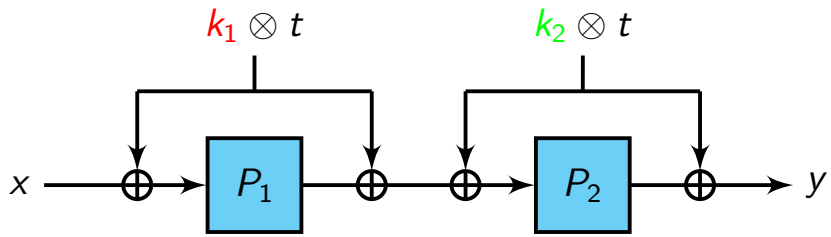
Conclusion

$2^{2n/3}$-secure constructions:

1. linear TKS



2. nonlinear TKS



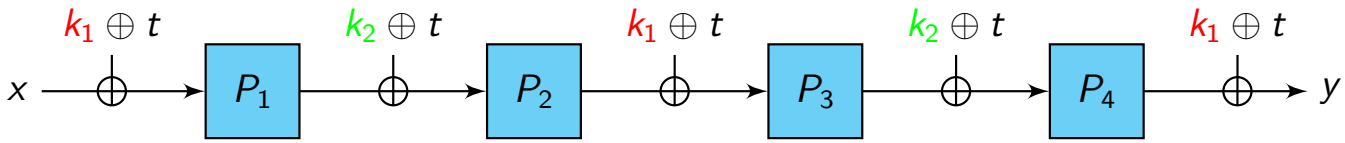
Open problems:

1. prove tight $2^{\frac{rn}{r+1}}$-security for r-round NL-TEM, $r \geq 3$
2. propose a construction with linear TKS and security $> 2^{2n/3}$
3. reduce key length for BBB-security

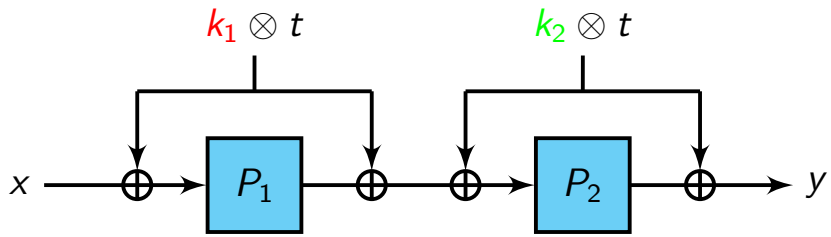
Conclusion

$2^{2n/3}$-secure constructions:

1. linear TKS



2. nonlinear TKS



Open problems:

1. prove tight $2^{\frac{rn}{r+1}}$-security for r-round NL-TEM, $r \geq 3$
2. propose a construction with linear TKS and security $> 2^{2n/3}$
3. reduce key length for BBB-security

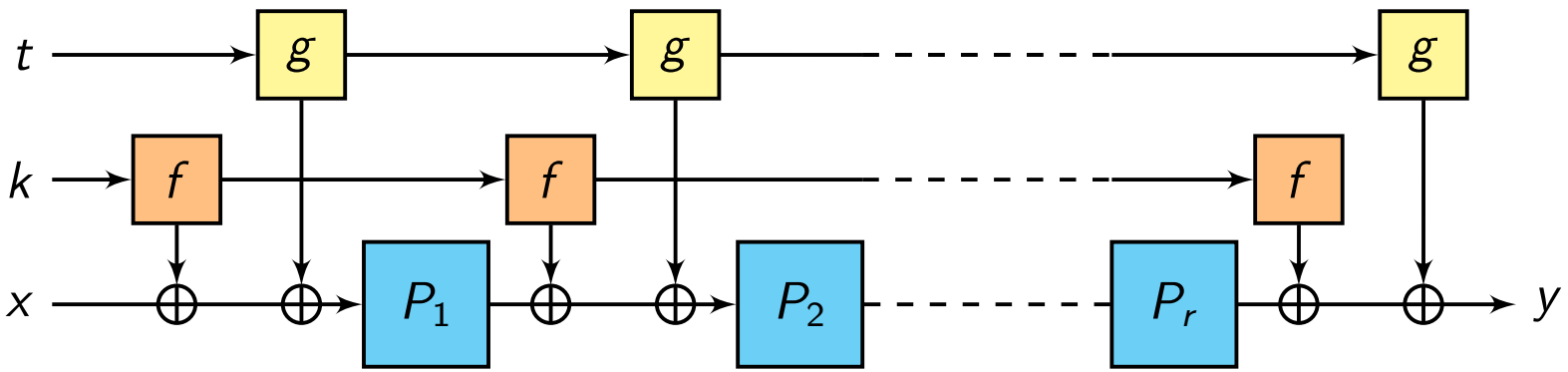
Link with the TWEAKEY Framework

- proposed by Jean, Nikolić, and Peyrin [JNP14]
- Superposition TWEAKEY (STK) constructions:

- sufficient conditions on f and g to have provable beyond-birthday-bound security in the RPM?
- NB: $f = g$ linear does not work since $\widetilde{E}(k, t, x) = E(k \oplus t, x)$

Link with the TWEAKEY Framework

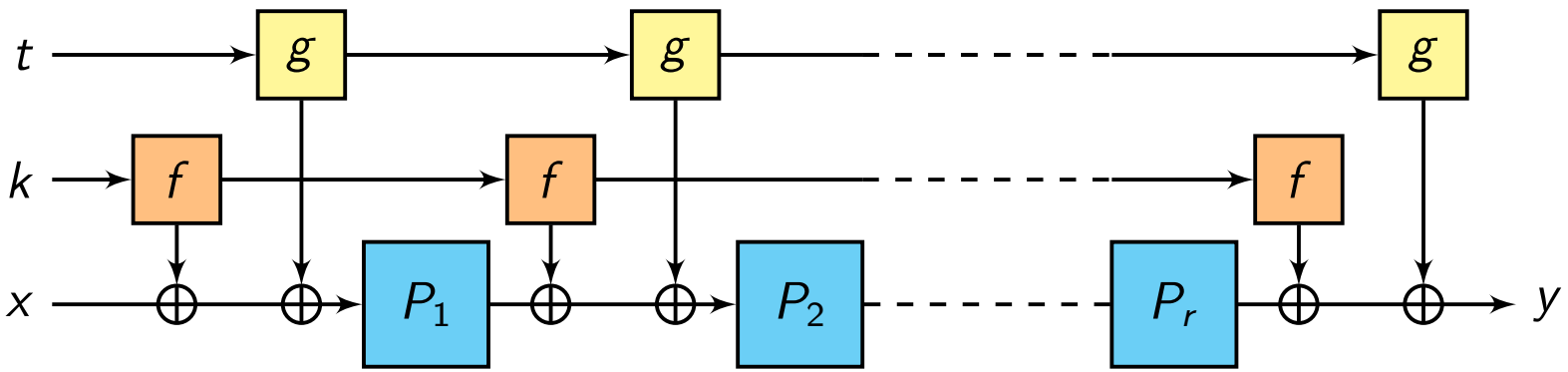
- proposed by Jean, Nikolić, and Peyrin [JNP14]
- Superposition TWEAKEY (STK) constructions:



- sufficient conditions on f and g to have provable beyond-birthday-bound security in the RPM?
- NB: $f = g$ linear does not work since $\widetilde{E}(k, t, x) = E(k \oplus t, x)$

Link with the TWEAKEY Framework

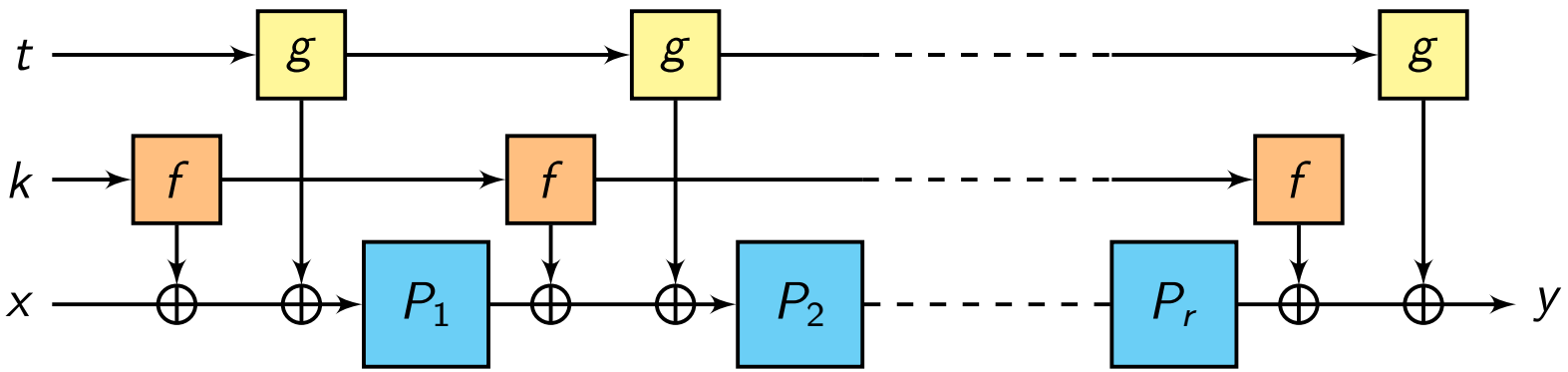
- proposed by Jean, Nikolić, and Peyrin [JNP14]
- Superposition TWEAKEY (STK) constructions:



- sufficient conditions on f and g to have provable beyond-birthday-bound security in the RPM?
- NB: $f = g$ linear does not work since $\widetilde{E}(k, t, x) = E(k \oplus t, x)$

Link with the TWEAKEY Framework

- proposed by Jean, Nikolić, and Peyrin [JNP14]
- Superposition TWEAKEY (STK) constructions:



- sufficient conditions on f and g to have provable beyond-birthday-bound security in the RPM?
- NB: $f = g$ linear does not work since $\widetilde{E}(k, t, x) = E(k \oplus t, x)$

The end...

Thanks for your attention!

Comments or questions?

References I

Benoît Cogliati, Rodolphe Lampe, and Yannick Seurin. Tweaking Even-Mansour Ciphers. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - Proceedings, Part I*, volume 9215 of *LNCS*, pages 189–208. Springer, 2015. Full version available at `http://eprint.iacr.org/2015/539`.

Paul Crowley. Mercy: A Fast Large Block Cipher for Disk Sector Encryption. In Bruce Schneier, editor, *Fast Software Encryption - FSE 2000*, volume 1978 of *LNCS*, pages 49–63. Springer, 2000.

Benoît Cogliati and Yannick Seurin. On the Provable Security of the Iterated Even-Mansour Cipher against Related-Key and Chosen-Key Attacks. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - Proceedings, Part I*, volume 9056 of *LNCS*, pages 584–613. Springer, 2015. Full version available at `http://eprint.iacr.org/2015/069`.

Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The Skein Hash Function Family. SHA3 Submission to NIST (Round 3), 2010.

References II

Pooya Farshim and Gordon Procter. The Related-Key Security of Iterated Even-Mansour Ciphers. In Gregor Leander, editor, *Fast Software Encryption - FSE 2015*, volume 9054 of *LNCS*, pages 342–363. Springer, 2015. Full version available at `http://eprint.iacr.org/2014/953`.

David Goldenberg, Susan Hohenberger, Moses Liskov, Elizabeth Crump Schwartz, and Hakan Seyalioglu. On Tweaking Luby-Rackoff Blockciphers. In Kaoru Kurosawa, editor, *Advances in Cryptology - ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 342–356. Springer, 2007.

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

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

References III


Rodolphe Lampe and Yannick Seurin. Tweakable Blockciphers with Asymptotically Optimal Security. In Shiho Moriai, editor, *Fast Software Encryption - FSE 2013*, volume 8424 of *LNCS*, pages 133–151. Springer, 2013.


Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable Blockciphers with Beyond Birthday-Bound Security. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012*, volume 7417 of *LNCS*, pages 14–30. Springer, 2012. Full version available at `http://eprint.iacr.org/2012/450`.


Bart Mennink. Optimally Secure Tweakable Blockciphers. In Gregor Leander, editor, *Fast Software Encryption - FSE 2015*, volume 9054 of *LNCS*, pages 428–448. Springer, 2015. Full version available at `http://eprint.iacr.org/2015/363`.


Atsushi Mitsuda and Tetsu Iwata. Tweakable Pseudorandom Permutation from Generalized Feistel Structure. In Joonsang Baek, Feng Bao, Kefei Chen, and Xuejia Lai, editors, *ProvSec 2008*, volume 5324 of *LNCS*, pages 22–37. Springer, 2008.

References IV


Kazuhiko Minematsu. Beyond-Birthday-Bound Security Based on Tweakable Block Cipher. In Orr Dunkelman, editor, *Fast Software Encryption - FSE 2009*, volume 5665 of *LNCS*, pages 308–326. Springer, 2009.


Phillip Rogaway. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. In Pil Joong Lee, editor, *Advances in Cryptology - ASIACRYPT 2004*, volume 3329 of *LNCS*, pages 16–31. Springer, 2004.


Richard Schroeppel. The Hasty Pudding Cipher. AES submission to NIST, 1998.