Tweaking Even-Mansour Ciphers

Benoît Cogliati[1] Rodolphe Lampe[1] Yannick Seurin[2]

[1]Versailles University, France

[2]ANSSI, France

August 17, 2015 — CRYPTO 2015

Outline

Background: Tweakable Block Ciphers

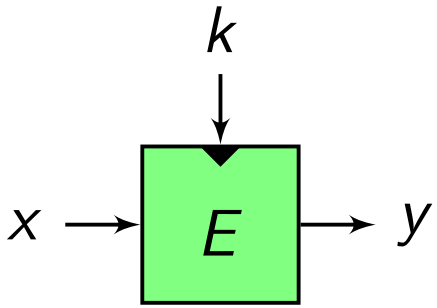
Our Contribution

Overview of the Proof for Two Rounds

Longer Cascades

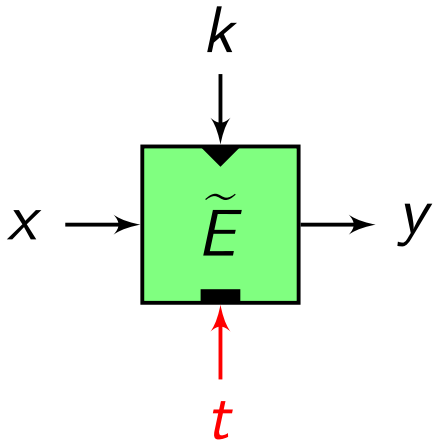
Conclusion and Perspectives

Tweakable Block Ciphers (TBCs)



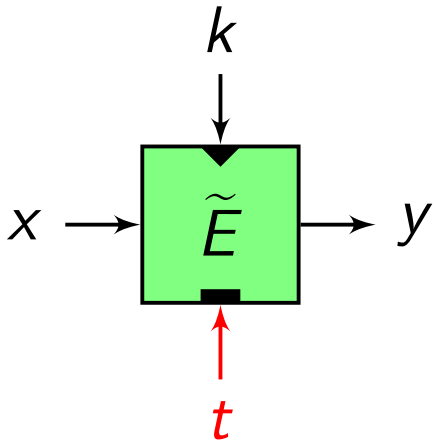
- tweak t: brings variability to the block cipher
- t assumed public or even adversarially controlled
- each tweak should give an "independent" permutation
- few "natively tweakable" BCs:
  - Hasty Pudding Cipher [Sch98]
  - Mercy [Cro00]
  - Threefish [FLS+10]
  - CAESAR proposals KIASU, Deoxys, Joltik,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

Tweakable Block Ciphers (TBCs)



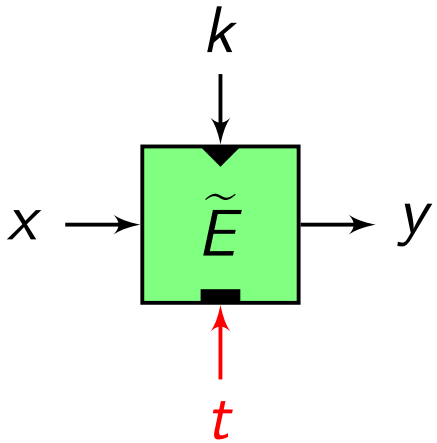
- tweak t: brings variability to the block cipher
- t assumed public or even adversarially controlled
- each tweak should give an "independent" permutation
- few "natively tweakable" BCs:
  - Hasty Pudding Cipher [Sch98]
  - Mercy [Cro00]
  - Threefish [FLS+10]
  - CAESAR proposals KIASU, Deoxys, Joltik,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

Tweakable Block Ciphers (TBCs)



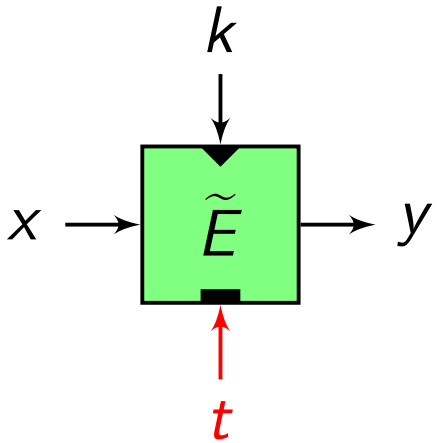
- tweak t: brings variability to the block cipher
- t assumed public or even adversarially controlled
- each tweak should give an "independent" permutation
- few "natively tweakable" BCs:
  - Hasty Pudding Cipher [Sch98]
  - Mercy [Cro00]
  - Threefish [FLS+10]
  - CAESAR proposals KIASU, Deoxys, Joltik,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

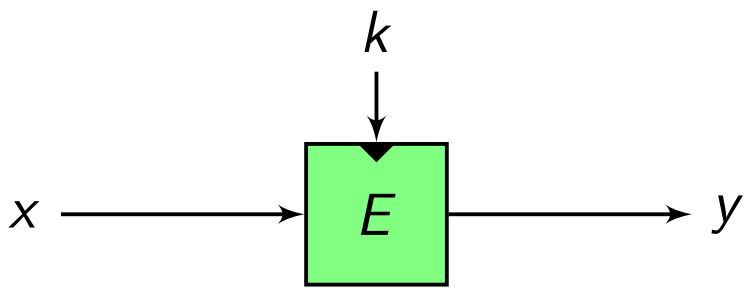
Generic Constructions of TBCs

- 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

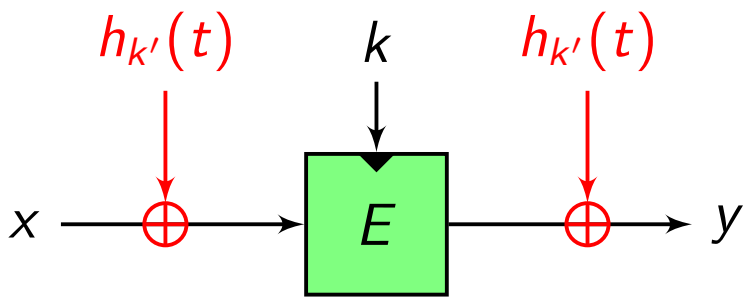
- A generic TBC construction turns a conventional block cipher E into a TBC $\widetilde{E}$
- example: LRW construction by Liskov *et al.* [LRW02]



- 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

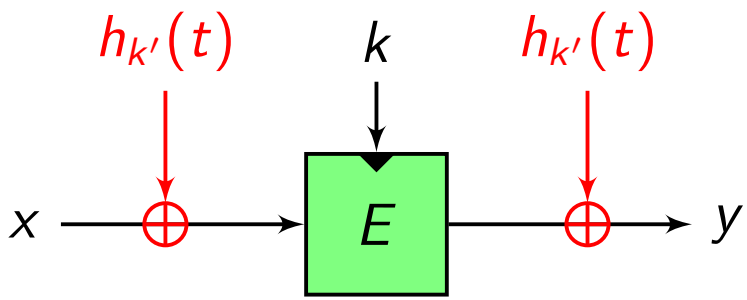
- A generic TBC construction turns a conventional block cipher E into a TBC $\widetilde{E}$
- example: LRW construction by Liskov *et al.* [LRW02]



- 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

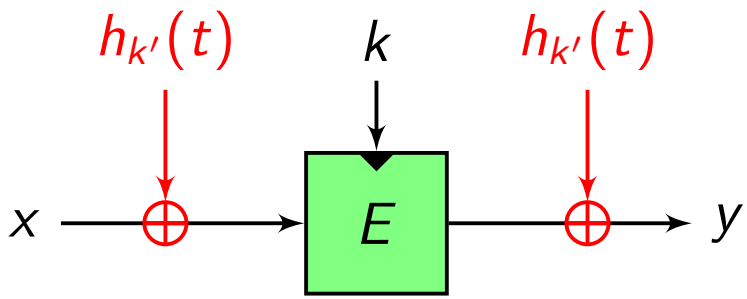
- A generic TBC construction turns a conventional block cipher E into a TBC $\widetilde{E}$
- example: LRW construction by Liskov *et al.* [LRW02]



- 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)

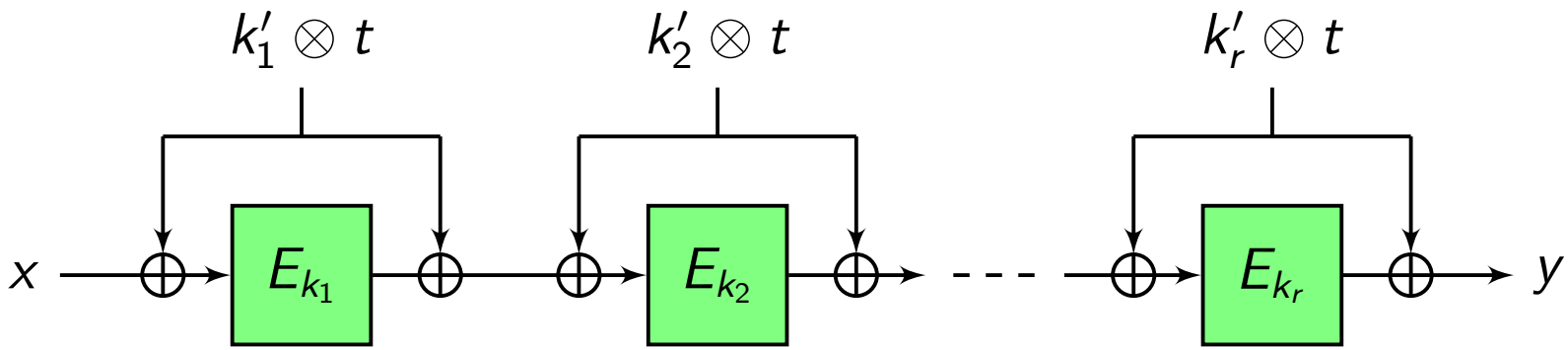
Generic Constructions of TBCs

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



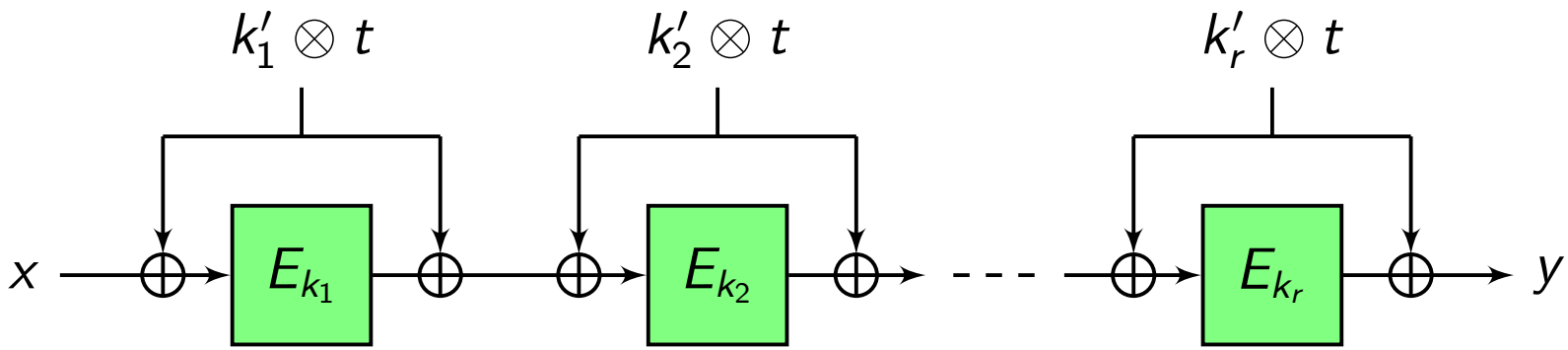
- h is XOR-universal, e.g. $h_{k'}(t) = k' \otimes t$ (field mult.)
- secure up to $\sim 2^{n/2}$ queries
- related construction XEX [Rog04] uses $E_k(t)$ instead of $h_{k'}(t)$ (used e.g. in the XTS disk encryption mode)

Cascading the LRW Construction



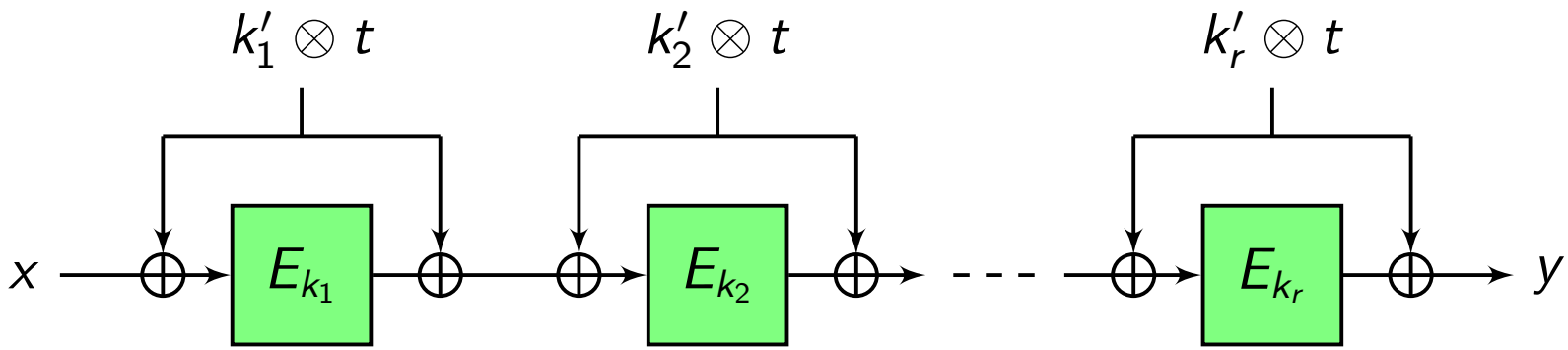
- $k_1, \ldots, k_r$ and $k'_1, \ldots, k'_r$ independent keys
  $\Rightarrow$ total key-length $= r(\kappa + n)$
- 2 rounds: provably secure up to $\sim 2^{2n/3}$ queries [LST12]
- r rounds, r even: provably secure up to $\sim 2^{\frac{rn}{r+2}}$ queries [LS13]
- NB: only assuming E is a PRP
  (standard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

Cascading the LRW Construction



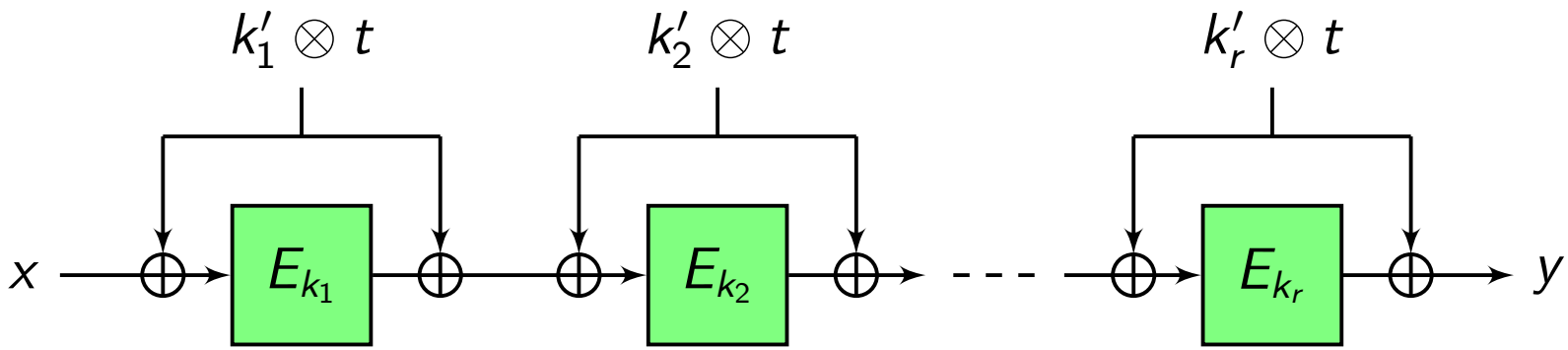
- $k_1, \ldots, k_r$ and $k'_1, \ldots, k'_r$ independent keys
  $\Rightarrow$ total key-length $= r(\kappa + n)$
- 2 rounds: provably secure up to $\sim 2^{2n/3}$ queries [LST12]
- r rounds, r even: provably secure up to $\sim 2^{\frac{rn}{r+2}}$ queries [LS13]
- NB: only assuming E is a PRP
  (standard 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)

Outline

Background: Tweakable Block Ciphers

Our Contribution

Overview of the Proof for Two Rounds

Longer Cascades

Conclusion and Perspectives

Tweakable Even-Mansour Constructions

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 work: SPN ciphers (more gen. key-alternating ciphers)

- analysis in the Random Permutation Model
  $\Rightarrow$ "tweakable" Even-Mansour construction(s)

Tweakable Even-Mansour Constructions

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 work: SPN ciphers (more gen. key-alternating ciphers)

- analysis in the Random Permutation Model
  $\Rightarrow$ "tweakable" Even-Mansour construction(s)

Tweakable Even-Mansour Constructions

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 work: SPN ciphers (more gen. key-alternating ciphers)

- analysis in the Random Permutation Model
  $\Rightarrow$ "tweakable" Even-Mansour construction(s)

Tweakable Even-Mansour Constructions

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 work: SPN ciphers (more gen. key-alternating ciphers)

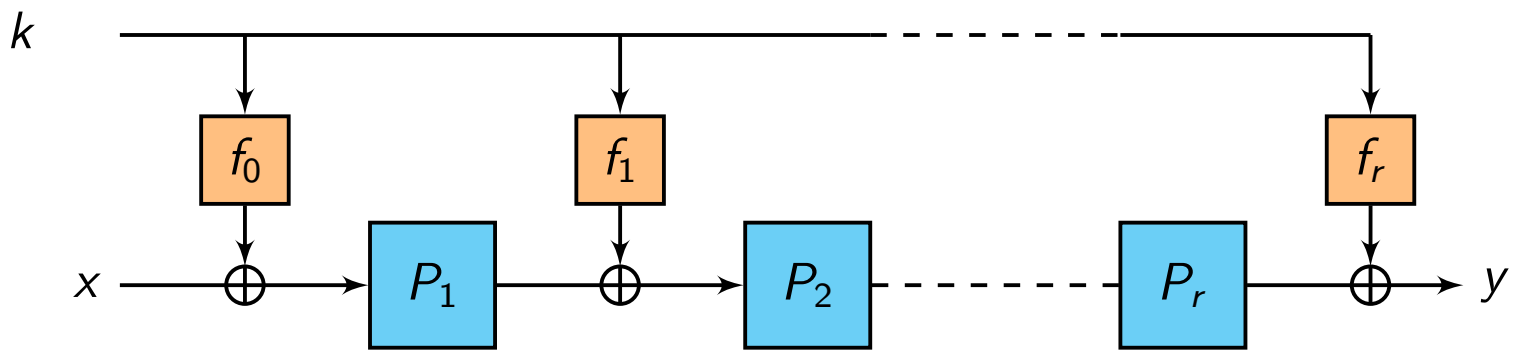
- analysis in the Random Permutation Model
  $\Rightarrow$ "tweakable" Even-Mansour construction(s)

Tweakable Even-Mansour Constructions

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 work: SPN ciphers (more gen. key-alternating ciphers)



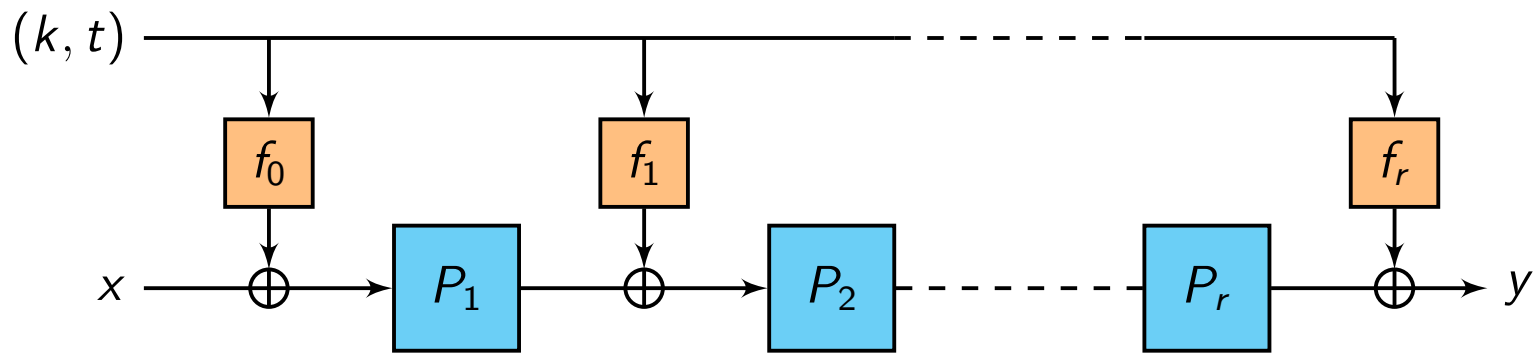
- analysis in the Random Permutation Model
  $\Rightarrow$ "tweakable" Even-Mansour construction(s)

Tweakable Even-Mansour Constructions

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 work: SPN ciphers (more gen. key-alternating ciphers)



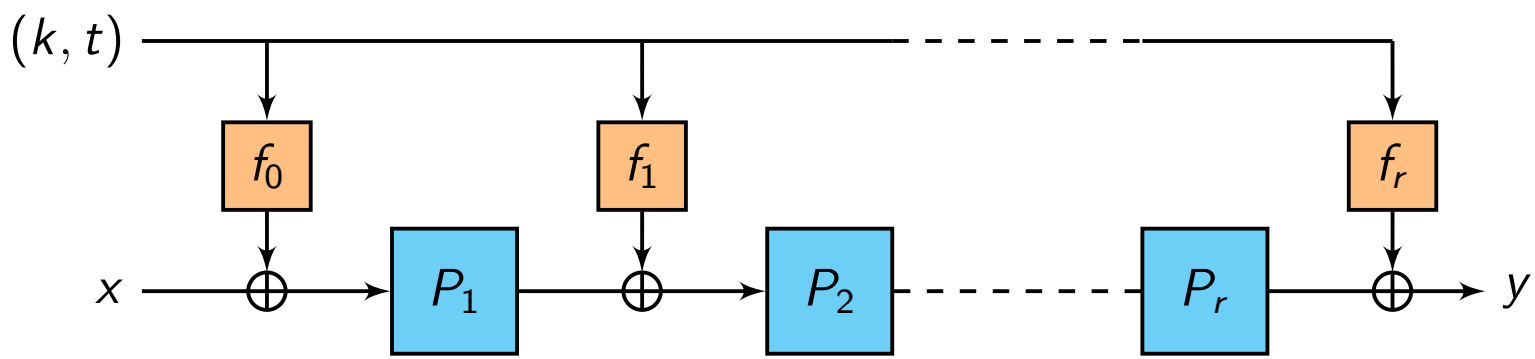
- analysis in the Random Permutation Model
  $\Rightarrow$ "tweakable" Even-Mansour construction(s)

Tweakable Even-Mansour Constructions

Our Goal

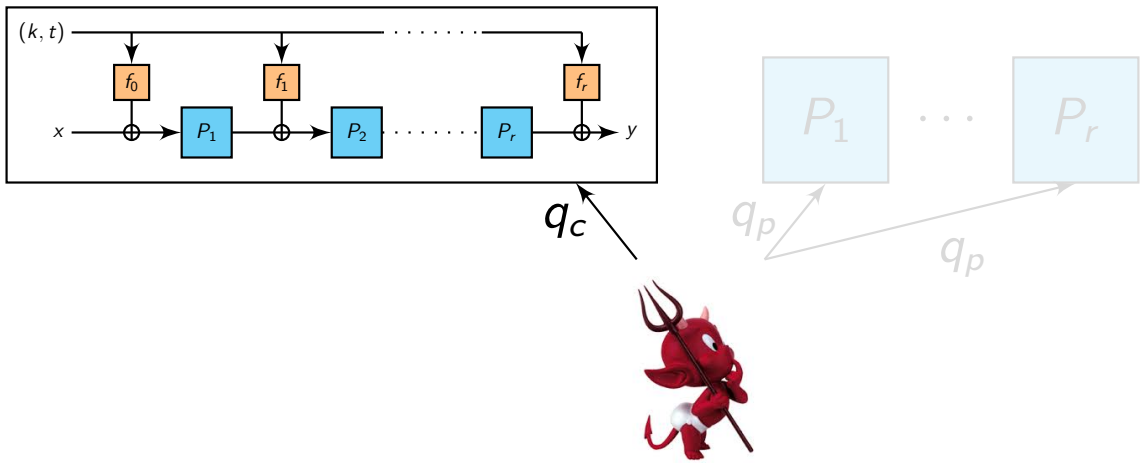
Provide provable security guidelines to design TBCs "from scratch" (rather than from an existing conventional block cipher).

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



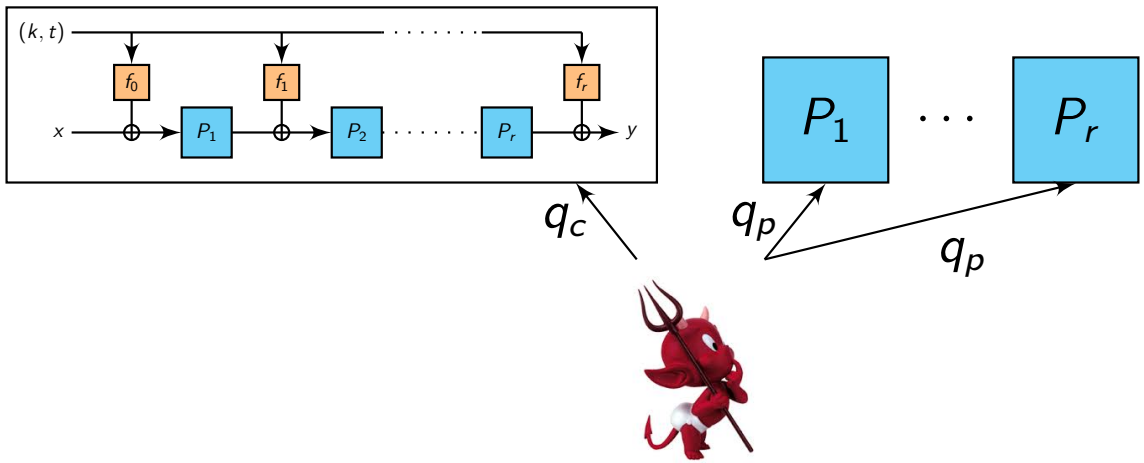
- analysis in the Random Permutation Model
  $\Rightarrow$ "tweakable" Even-Mansour construction(s)

The Random Permutation Model (RPM)



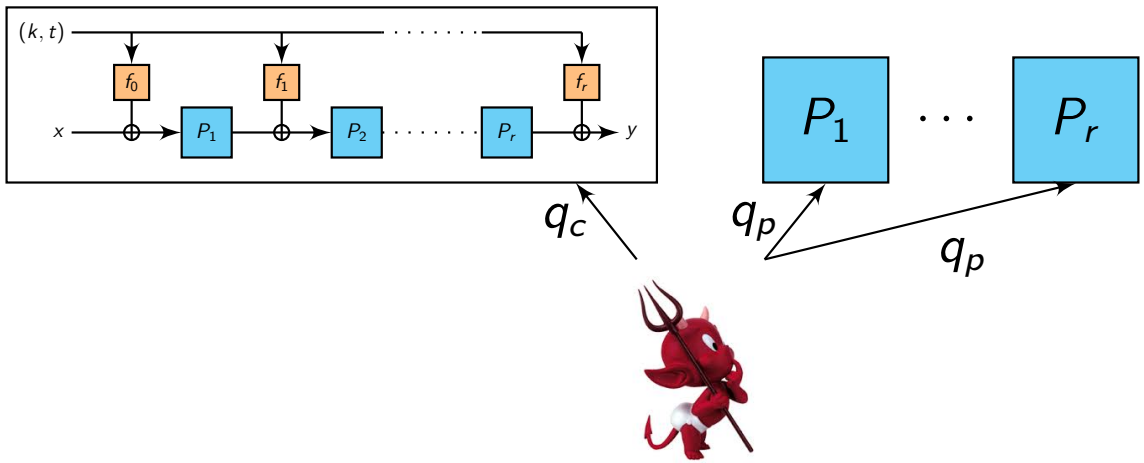
- the P_i's are modeled as public random permutation oracles (adversary can only make black-box queries)
- adversary cannot exploit any weakness of the P_i's
  $\Rightarrow$ generic attacks
- complexity measure of the adversary:
  - q_c = # construction queries = pt/ct pairs (data D)
  - q_p = # queries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

The Random Permutation Model (RPM)



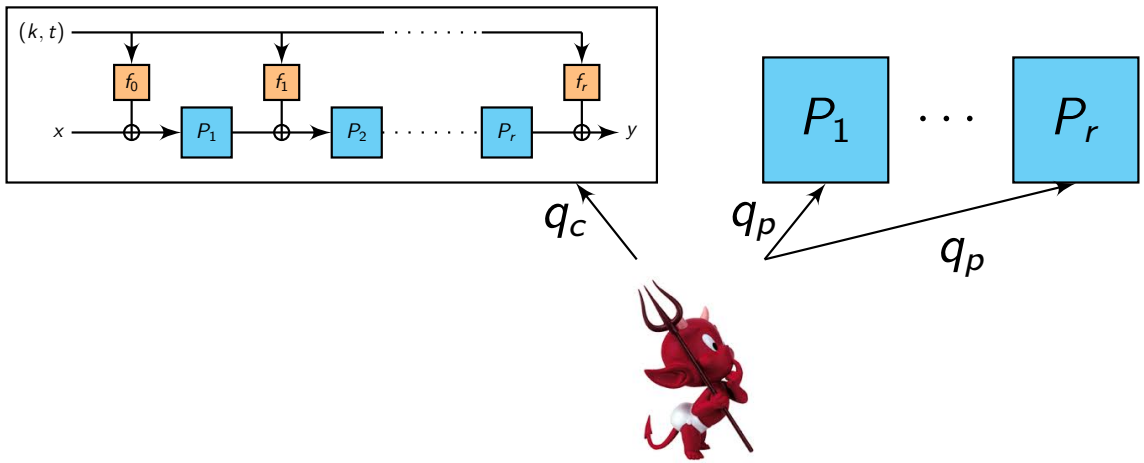
- the P_i's are modeled as public random permutation oracles (adversary can only make black-box queries)
- adversary cannot exploit any weakness of the P_i's
  $\Rightarrow$ generic attacks
- complexity measure of the adversary:
  - q_c = # construction queries = pt/ct pairs (data D)
  - q_p = # queries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

The Random Permutation Model (RPM)



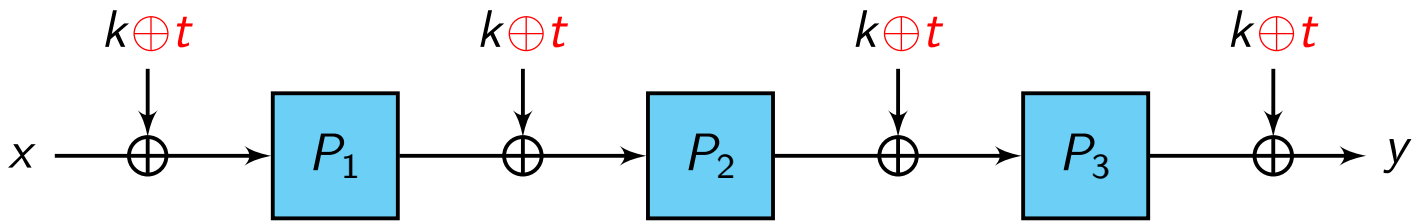
- the P_i's are modeled as public random permutation oracles (adversary can only make black-box queries)
- adversary cannot exploit any weakness of the P_i's
  $\Rightarrow$ generic attacks
- complexity measure of the adversary:
  - $q_c = \#$ construction queries $=$ pt/ct pairs (data D)
  - $q_p =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

The Random Permutation Model (RPM)



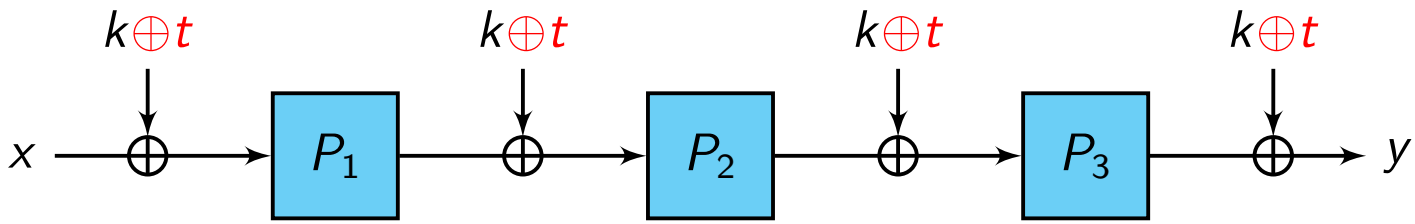
- the P_i's are modeled as public random permutation oracles (adversary can only make black-box queries)
- adversary cannot exploit any weakness of the P_i's
  $\Rightarrow$ generic attacks
- complexity measure of the adversary:
  - $q_c = \#$ construction queries $=$ pt/ct pairs (data D)
  - $q_p =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

Previous Result



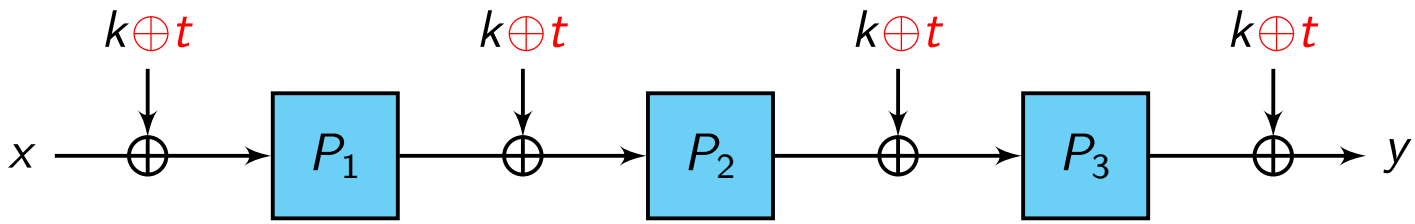
- provably secure in the RPM up to $\sim 2^{n/2}$ queries [CS15, FP15]
- can be written $\widetilde{E}(k, t, x) = E(k \oplus t, x)$ where E is the conventional 3-round EM cipher with trivial key-schedule
- $\Rightarrow$ secure up to $2^{n/2}$ queries *at best* by a simple collision attack

Previous Result



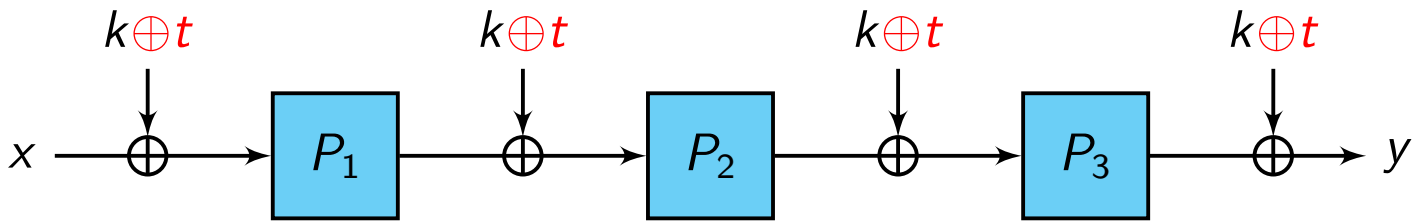
- provably secure in the RPM up to $\sim 2^{n/2}$ queries [CS15, FP15]
- can be written $\widetilde{E}(k, t, x) = E(k \oplus t, x)$ where E is the conventional 3-round EM cipher with trivial key-schedule
- $\Rightarrow$ secure up to $2^{n/2}$ queries *at best* by a simple collision attack

Previous Result



- provably secure in the RPM up to $\sim 2^{n/2}$ queries [CS15, FP15]
- 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

Previous Result



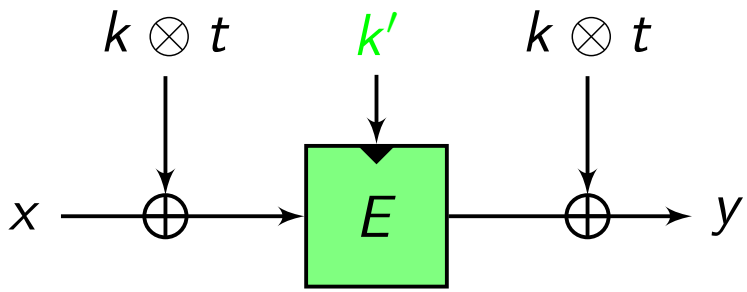
- provably secure in the RPM up to $\sim 2^{n/2}$ queries [CS15, FP15]
- can be written $\widetilde{E}(k, t, x) = E(k \oplus t, x)$ where E is the conventional 3-round EM cipher with trivial key-schedule
- $\Rightarrow$ secure up to $2^{n/2}$ queries *at best* by a simple collision attack

Question

How can we obtain a construction with security beyond the birthday-bound?

Back to LRW

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



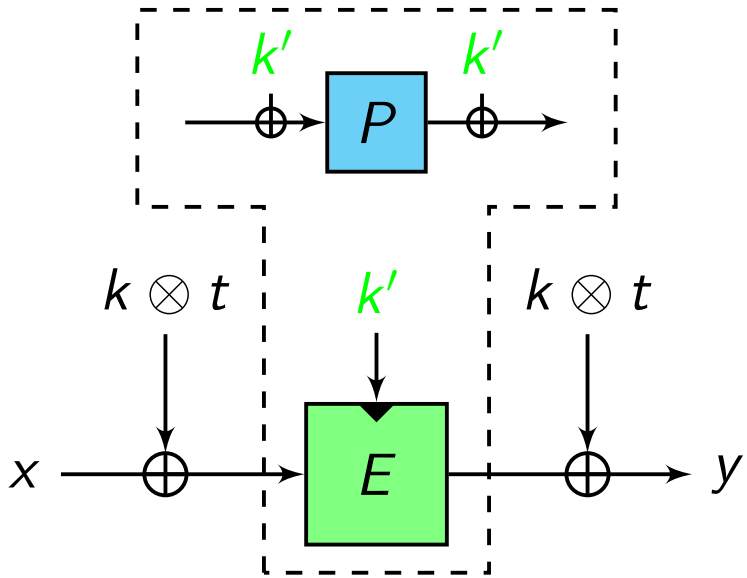
- provably secure in the RPM up to $\sim 2^{n/2}$ queries:

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

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

Back to LRW

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



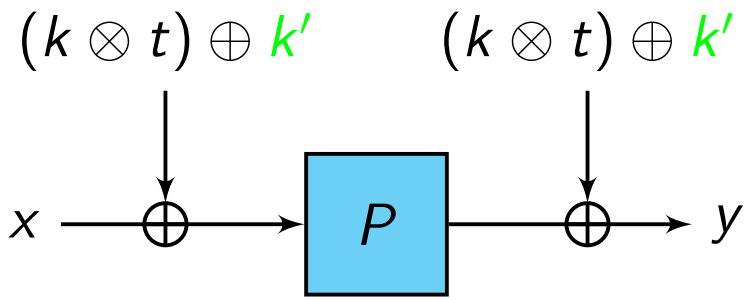
- provably secure in the RPM up to $\sim 2^{n/2}$ queries:

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

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

Back to LRW

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



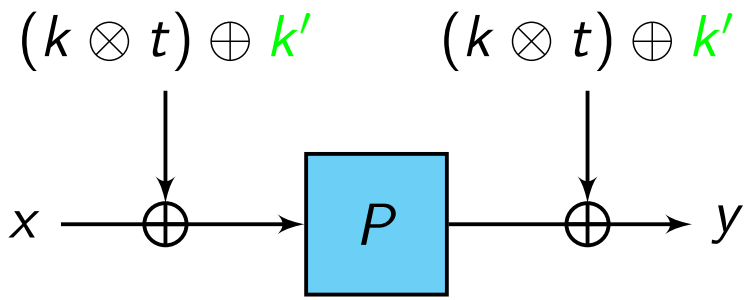
- provably secure in the RPM up to $\sim 2^{n/2}$ queries:

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

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

Back to LRW

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



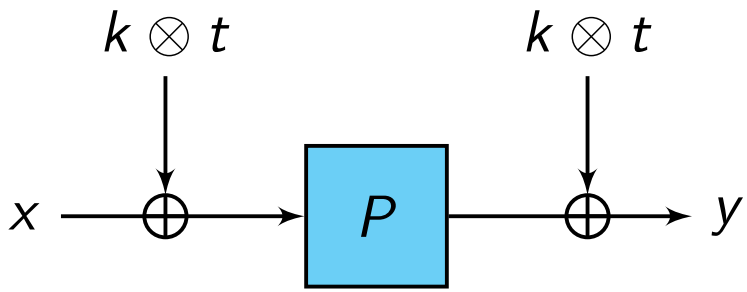
- provably secure in the RPM up to $\sim 2^{n/2}$ queries:

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

- $t \neq 0 \Rightarrow k'$ 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:

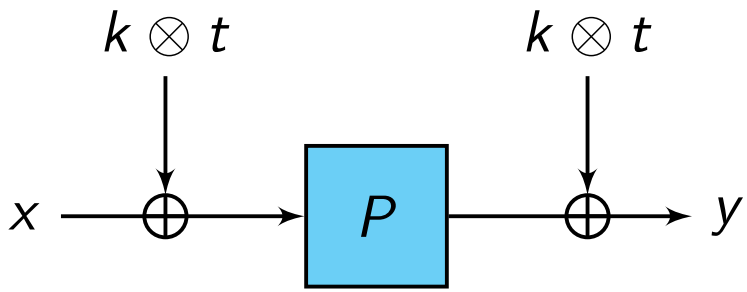
$$\mathbf{Adv}(q_c, q_p) \leq \frac{q_c^2}{2^n} + \frac{2q_c q_p}{2^n}.$$

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

Back to LRW

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

(1-round) Tweakable Even-Mansour (TEM) construction



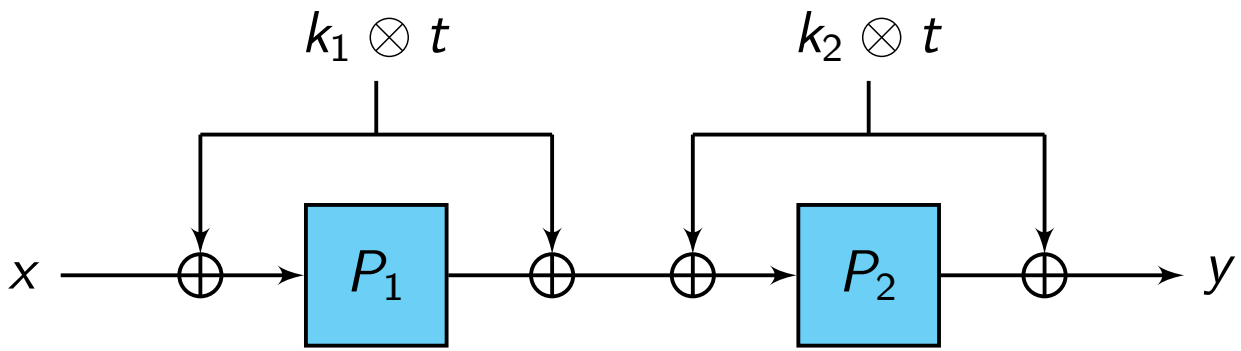
- provably secure in the RPM up to $\sim 2^{n/2}$ queries:

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

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

Cascading the TEM Construction

- k_1, k_2 independent n-bit keys

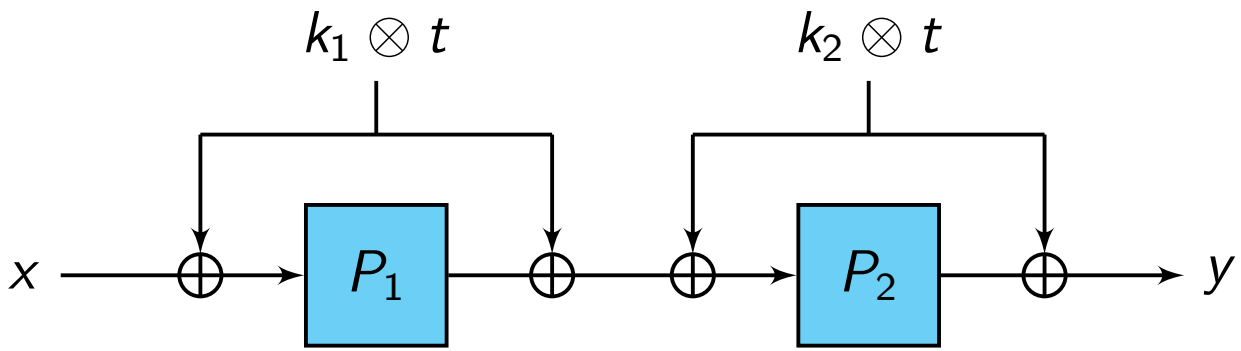


- our main result: secure up to $\sim 2^{2n/3}$ queries in the RPM:

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

Cascading the TEM Construction

- k_1, k_2 independent n-bit keys



- our main result: secure up to $\sim 2^{2n/3}$ queries in the RPM:

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

Outline

Background: Tweakable Block Ciphers

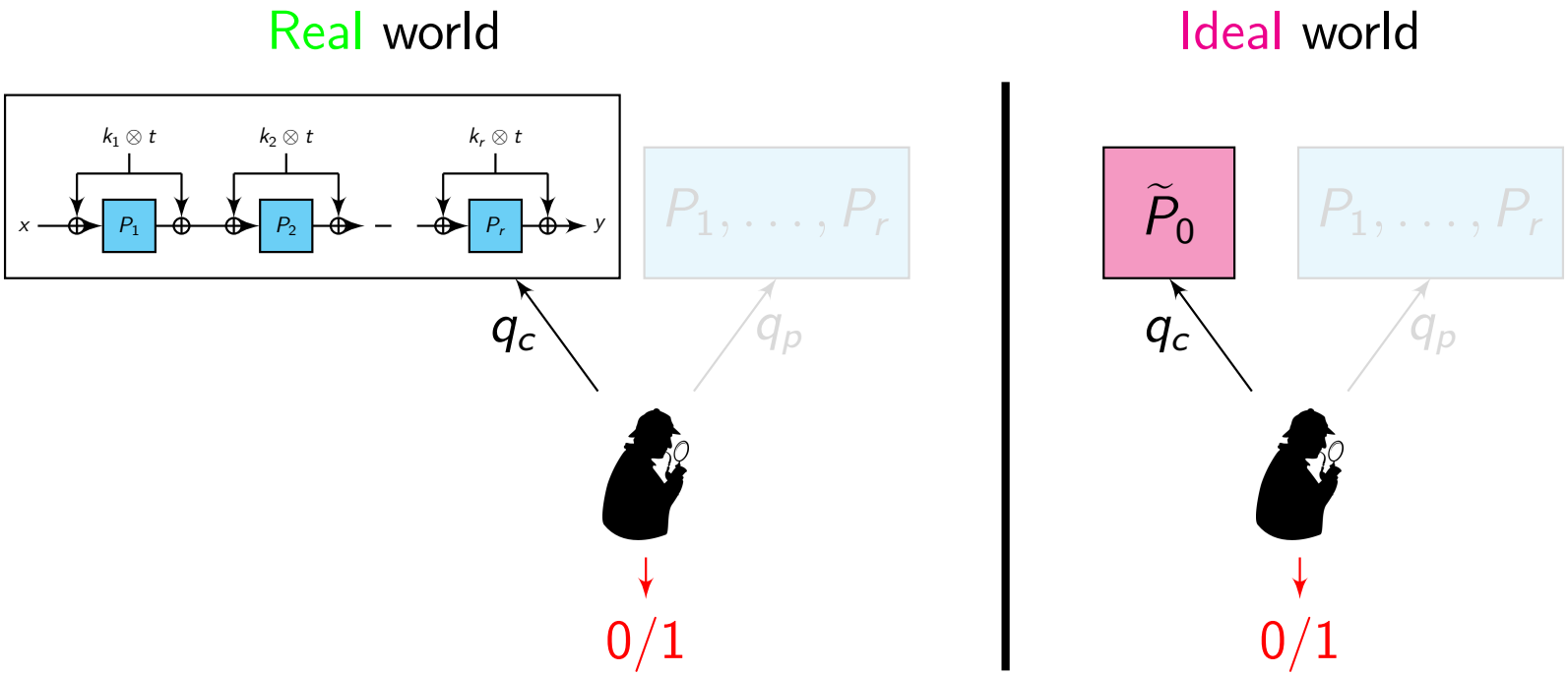
Our Contribution

Overview of the Proof for Two Rounds

Longer Cascades

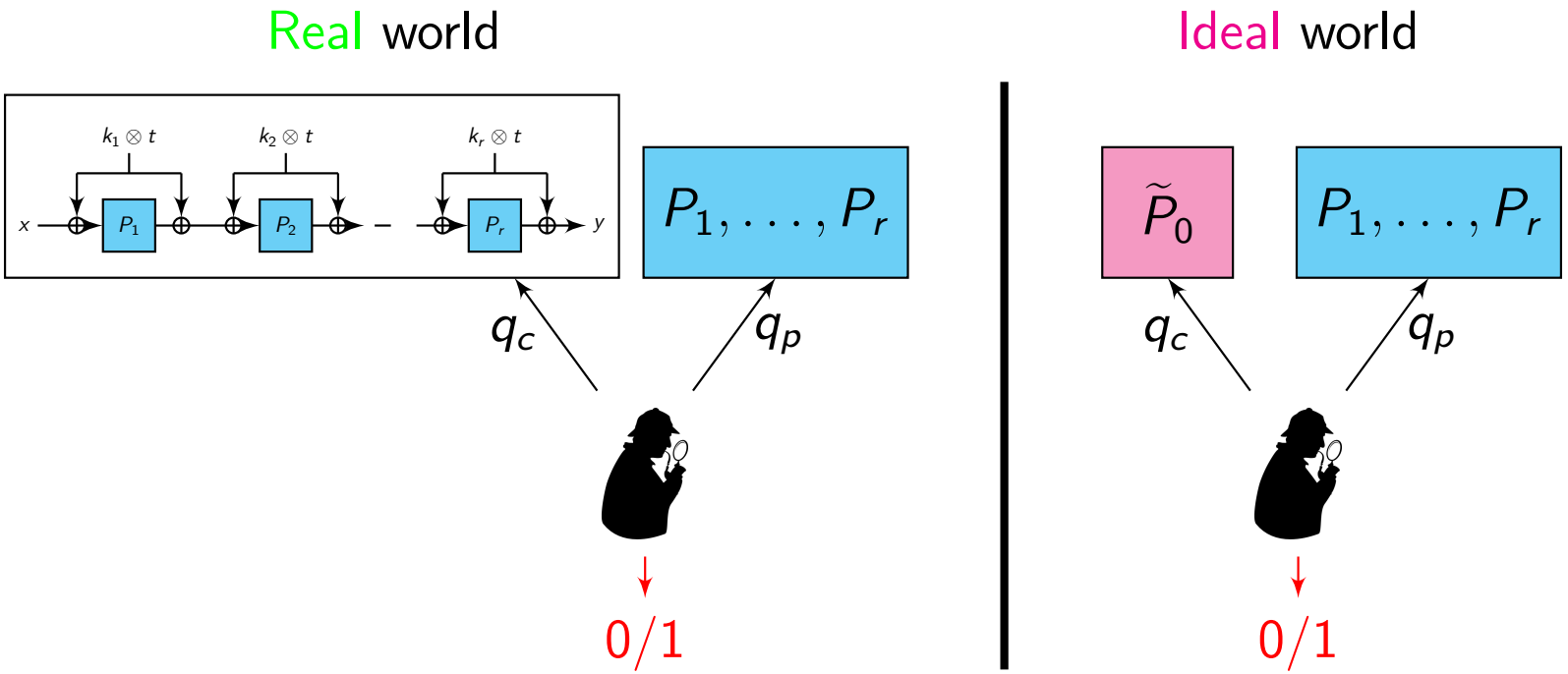
Conclusion and Perspectives

Formalization of the Security Experiment



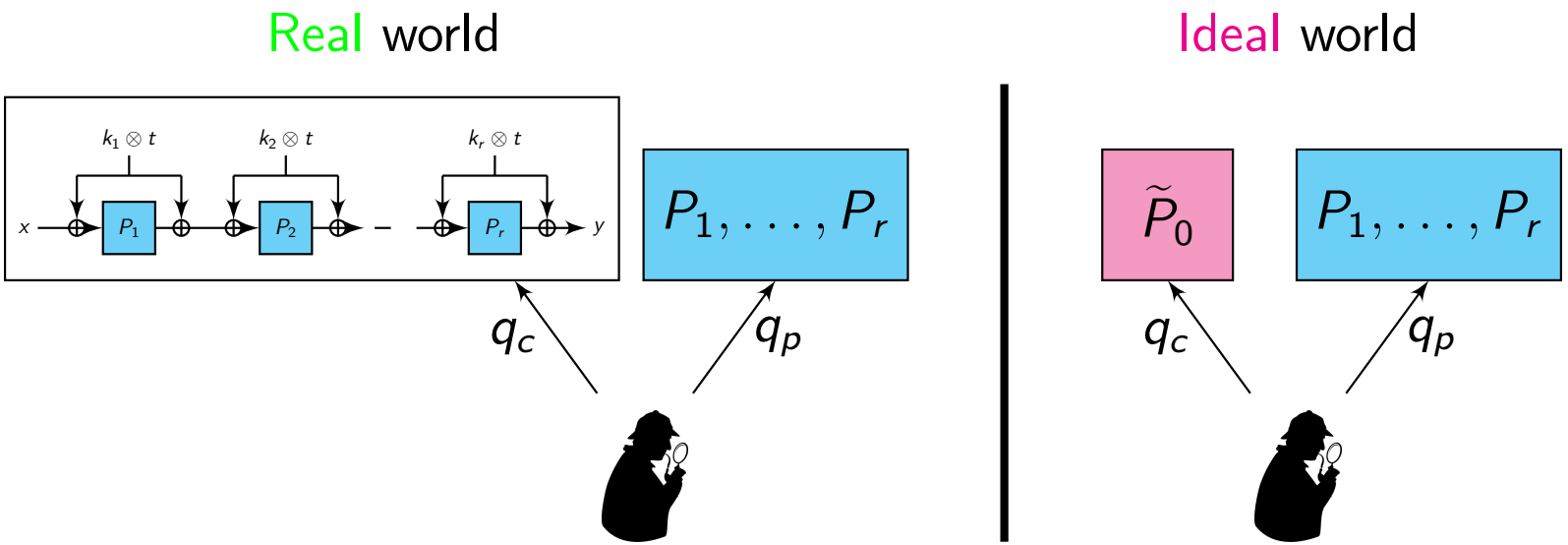
- real world: TEM construction with random keys $k_1, \ldots, k_r$
- ideal world: random tweakable permutation $\widetilde{P}_0$ independent from $P_1, \ldots, P_r$
- RPM: $\mathcal{D}$ has oracle access to $P_1, \ldots, P_r$ in both worlds

Formalization of the Security Experiment



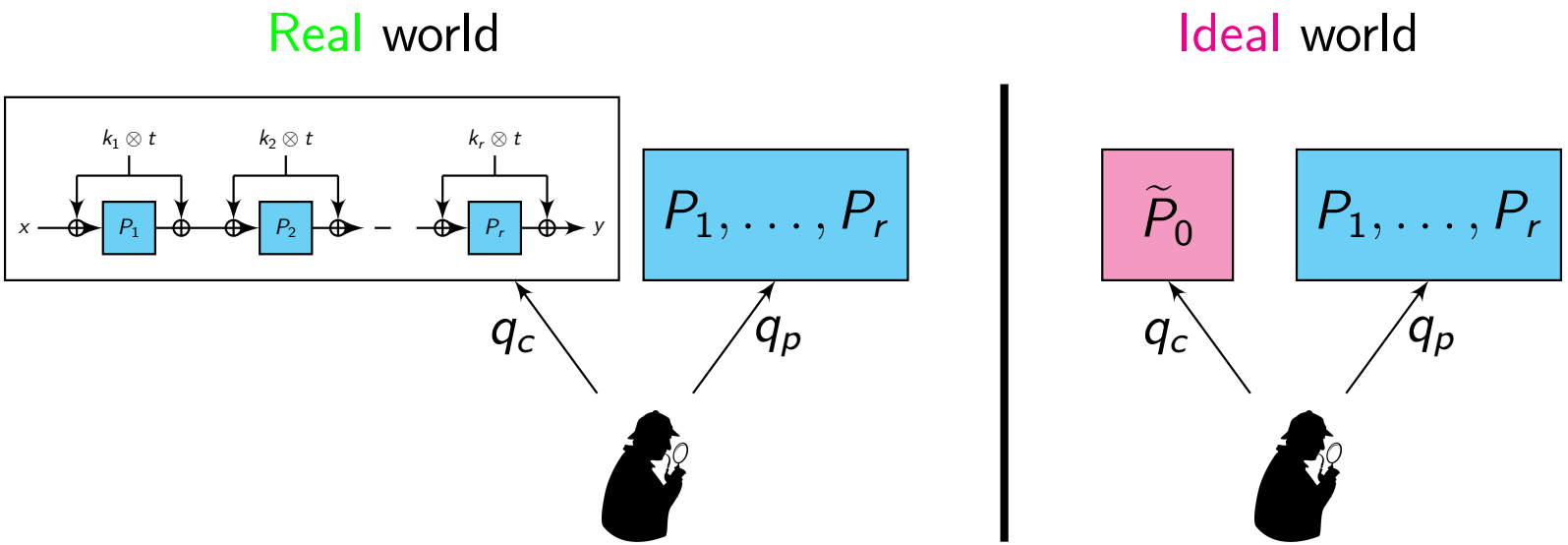
- real world: TEM construction with random keys $k_1, \ldots, k_r$
- ideal world: random tweakable permutation $\widetilde{P}_0$ independent from $P_1, \ldots, P_r$
- RPM: $\mathcal{D}$ has oracle access to $P_1, \ldots, P_r$ in both worlds

Proof Technique: H-coefficients



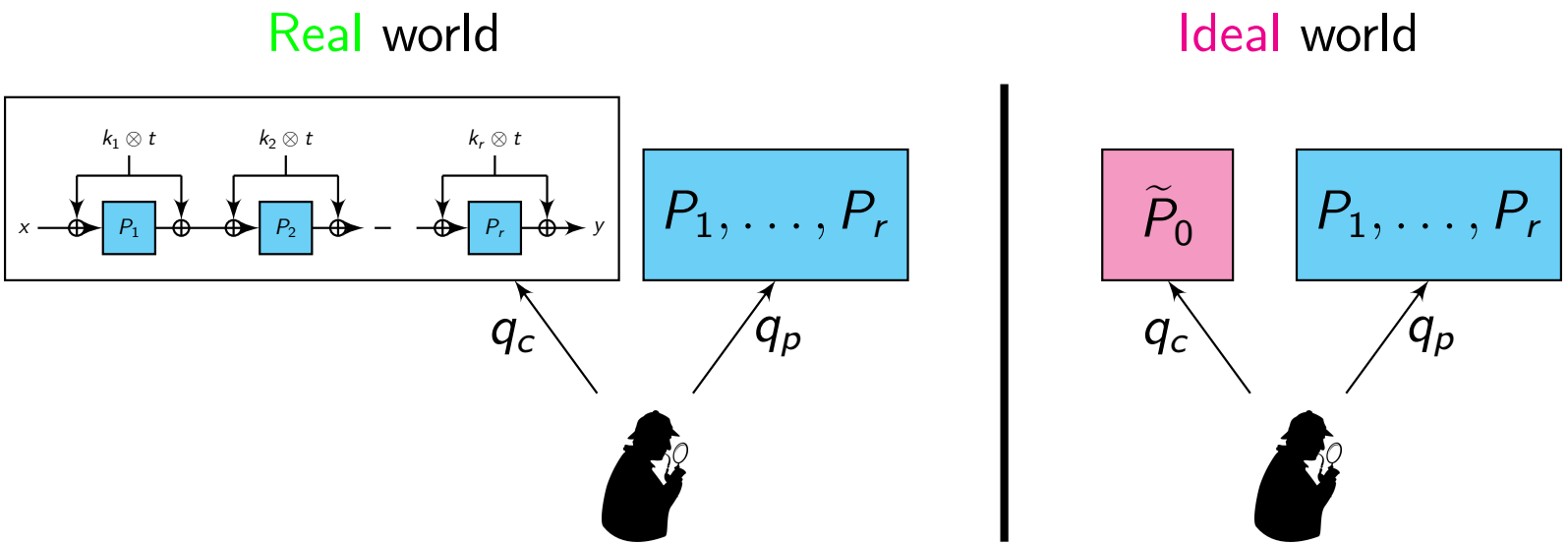
1. consider the transcript of all queries of $\mathcal{D}$ to the construction and to the inner permutations
2. define bad transcripts and show that their probability is small (in the ideal world)
3. show that good transcripts are almost as probable in the real and the ideal world

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

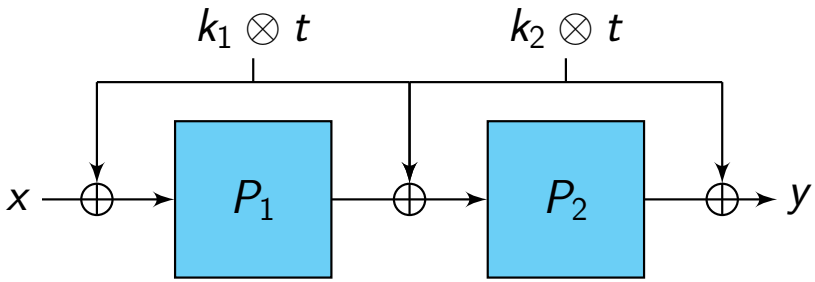
Proof Technique: H-coefficients



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

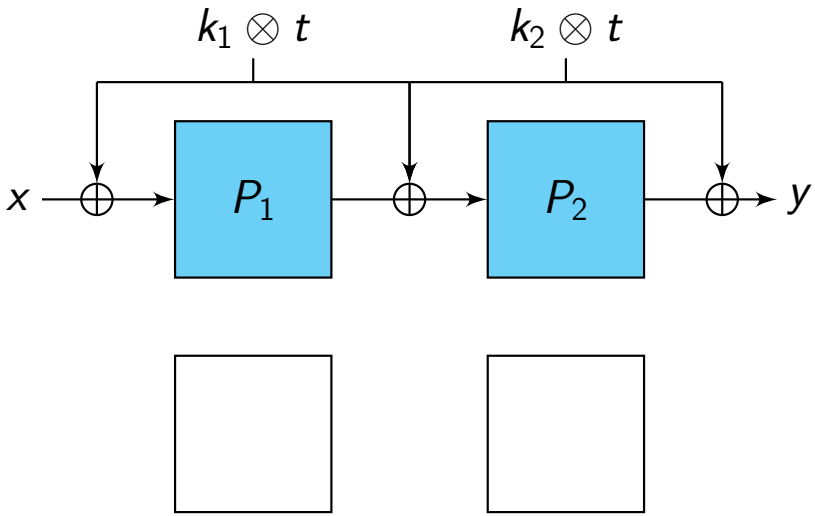
Bad Transcripts

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



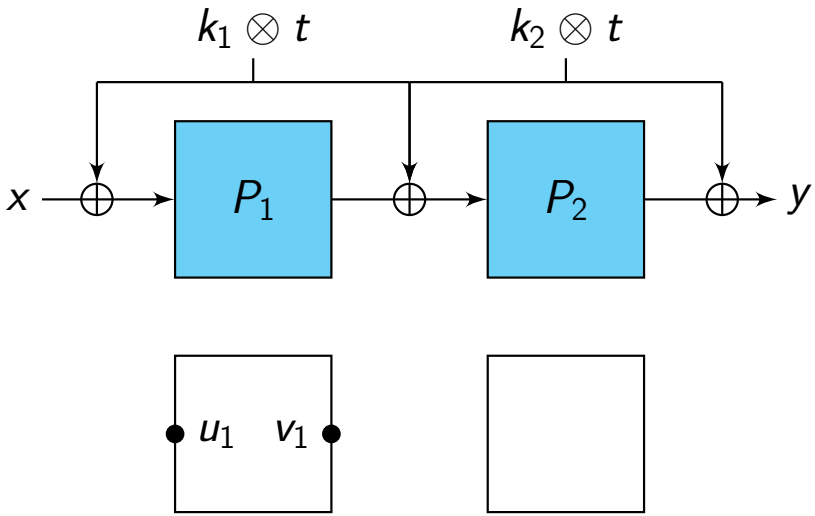
Bad Transcripts

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



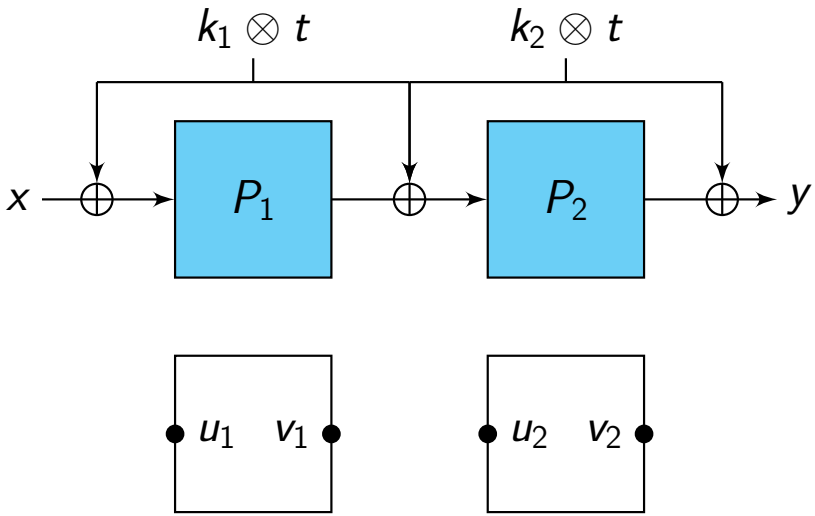
Bad Transcripts

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



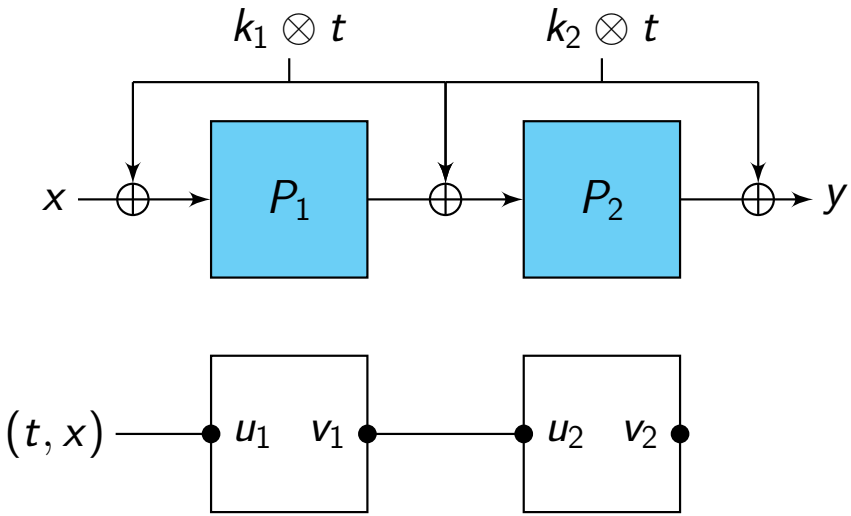
Bad Transcripts

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



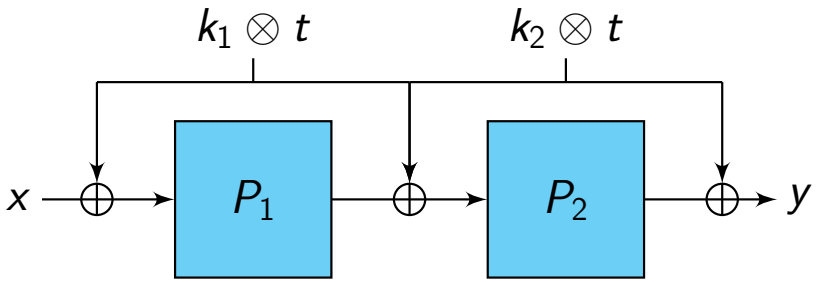
Bad Transcripts

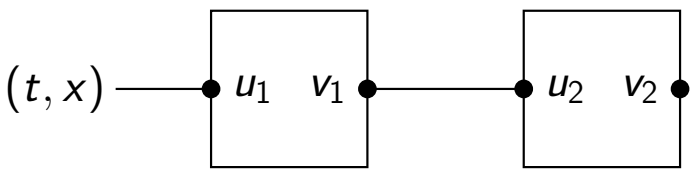
- one needs to avoid "two-fold" collisions:



Bad Transcripts

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

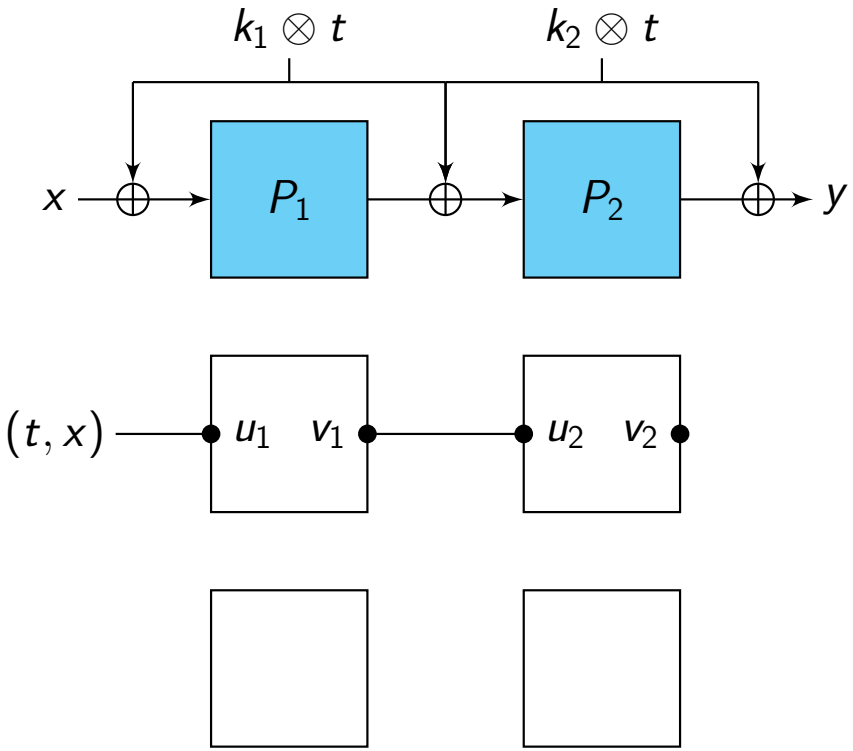




$$\text{proba} \leq \frac{q_c q_p^2}{2^{2n}}$$

Bad Transcripts

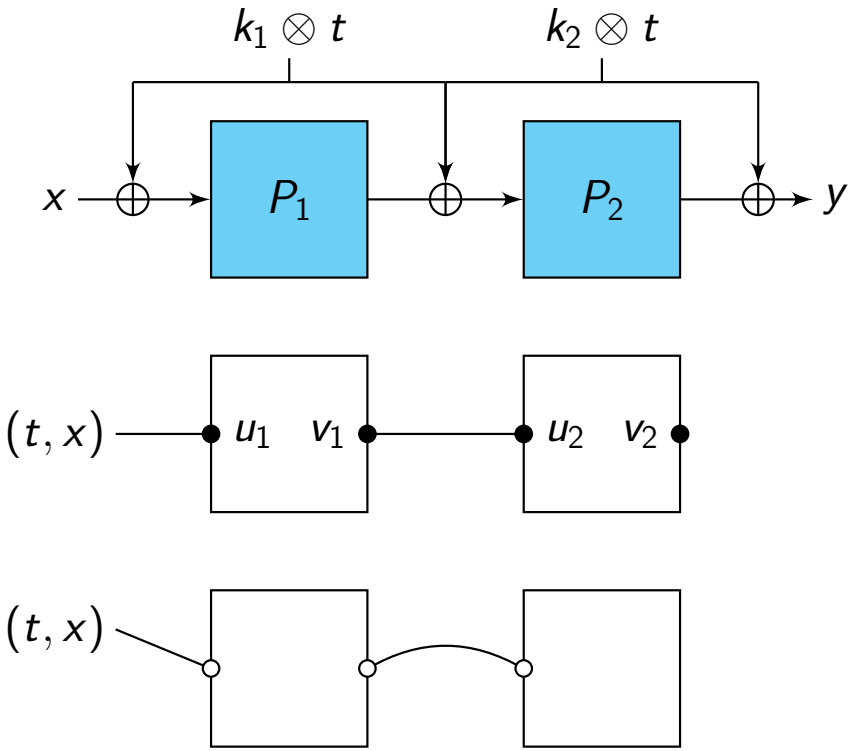
- one needs to avoid "two-fold" collisions:



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

Bad Transcripts

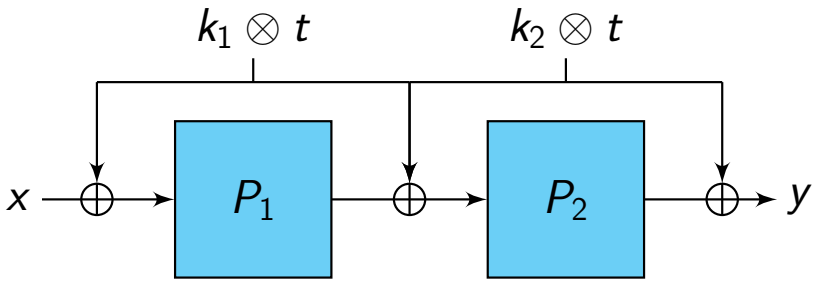
- one needs to avoid "two-fold" collisions:

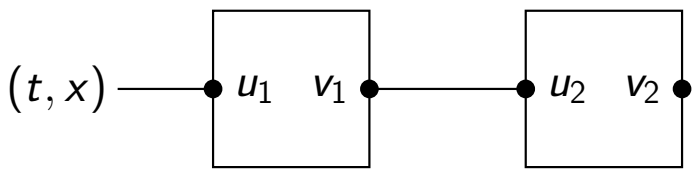


$$\text{proba} \leq \frac{q_c q_p^2}{2^{2n}}$$

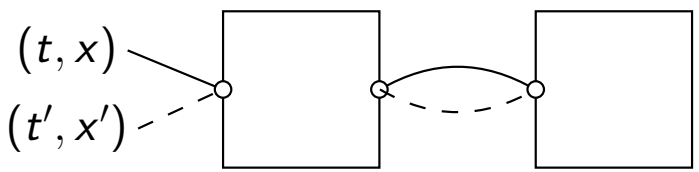
Bad Transcripts

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



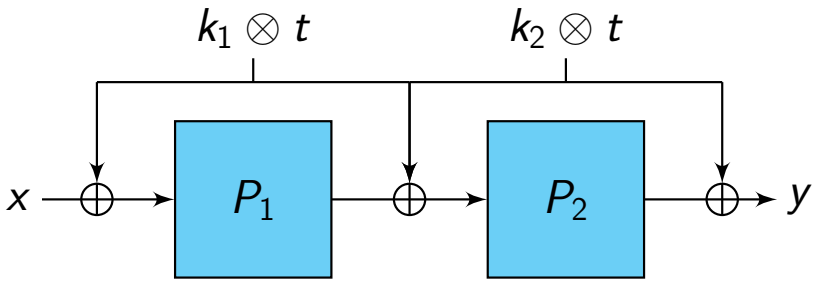


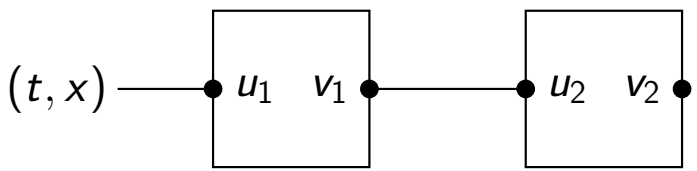
$$\text{proba} \leq \frac{q_c q_p^2}{2^{2n}}$$



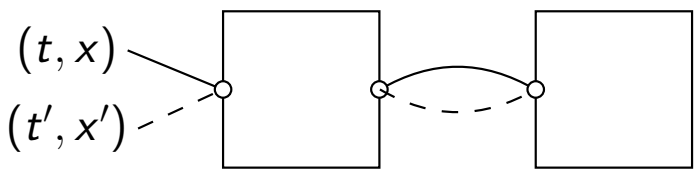
Bad Transcripts

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



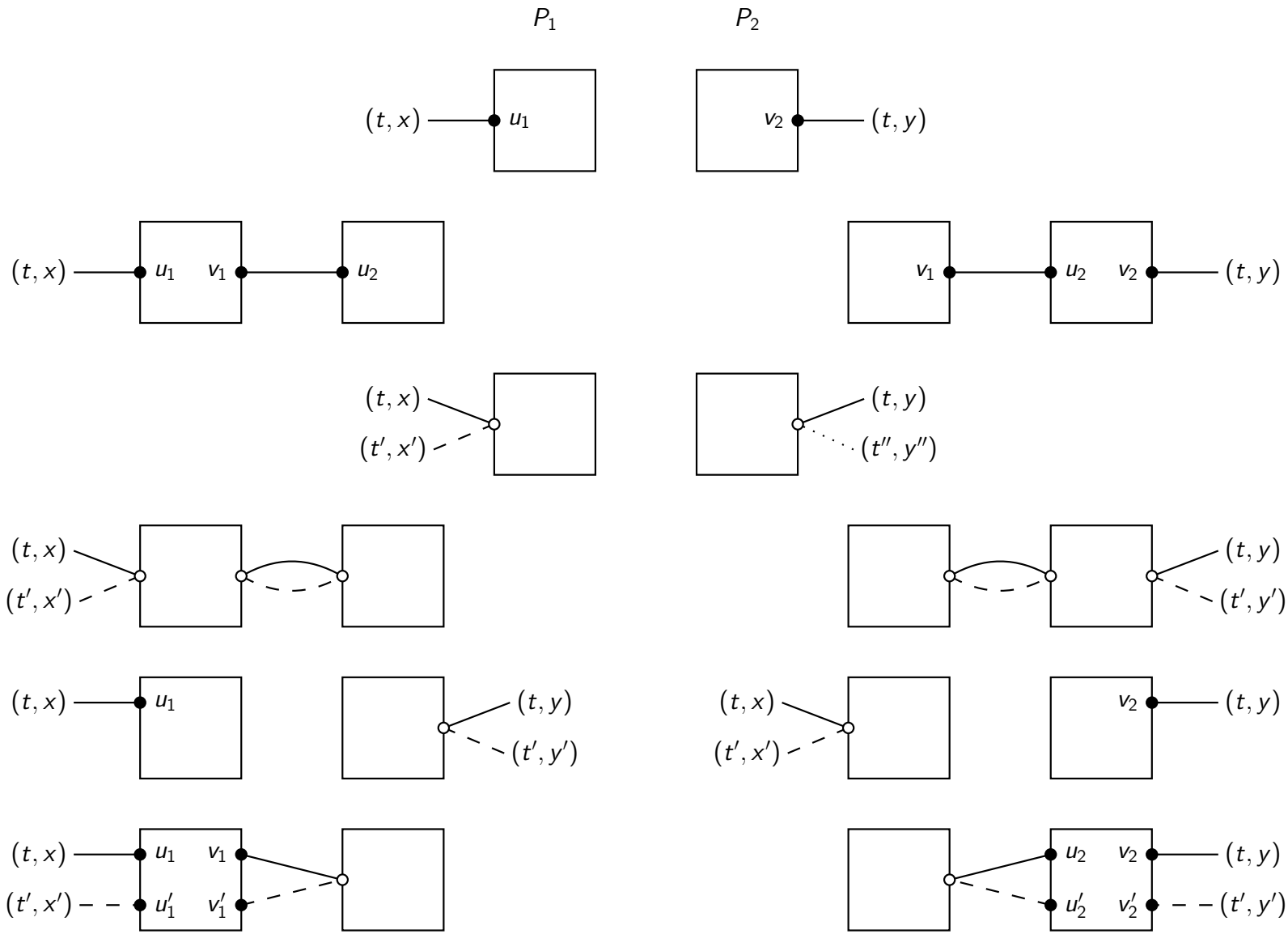


$$\text{proba} \leq \frac{q_c q_p^2}{2^{2n}}$$

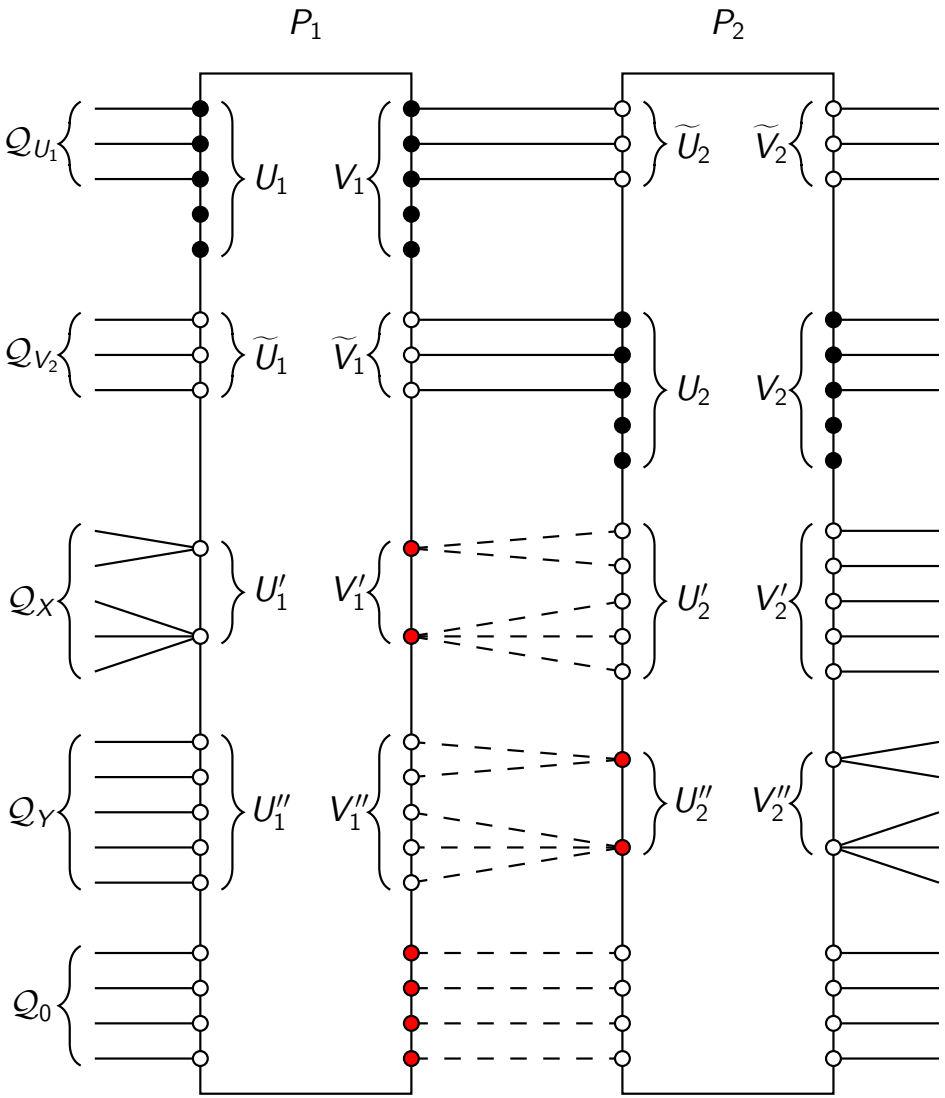


$$\text{proba} \leq \frac{q_c^2}{2^{2n}}$$

The Ten "Bad Collision" Cases

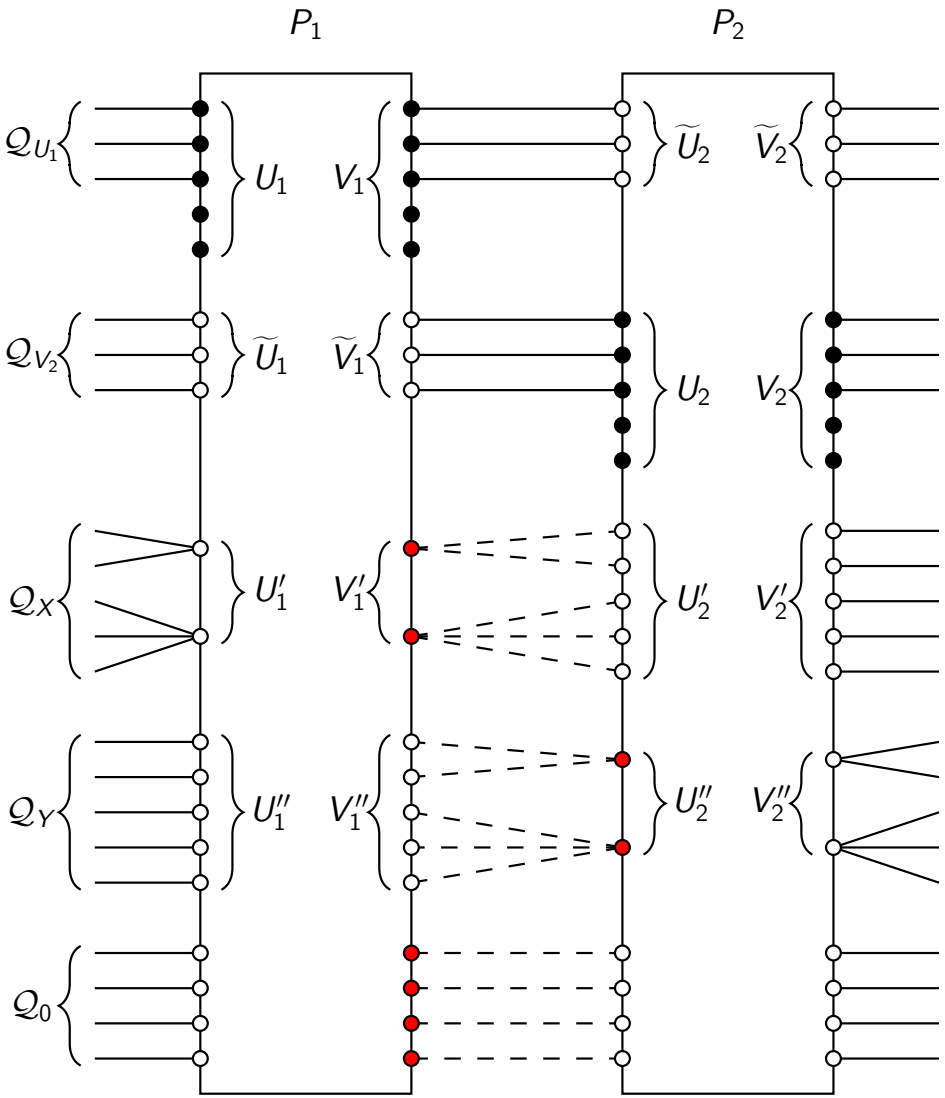


Distribution of Good Transcripts



- 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

Outline

Background: Tweakable Block Ciphers

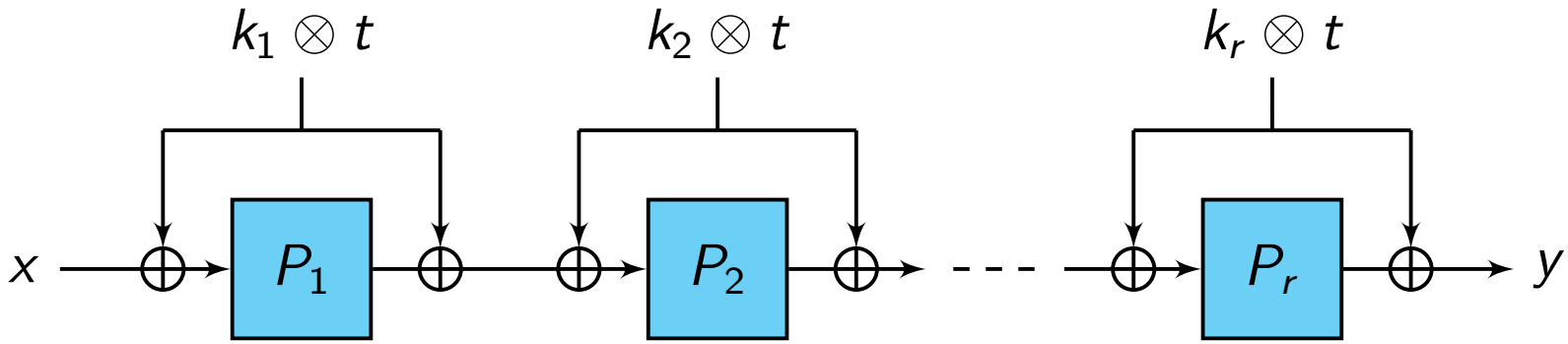
Our Contribution

Overview of the Proof for Two Rounds

Longer Cascades

Conclusion and Perspectives

Longer Cascades of the TEM Construction

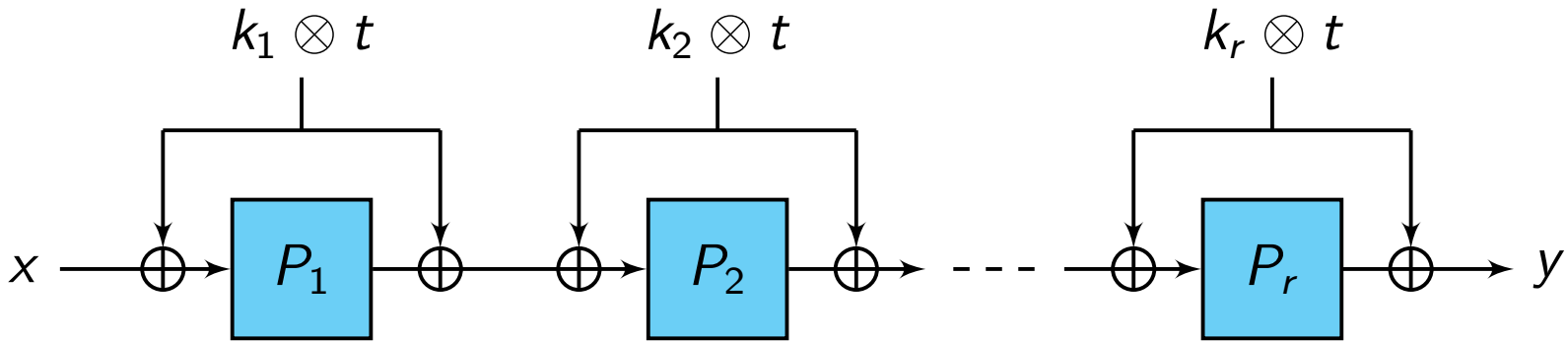


- r rounds, r even, with independent keys $k_1, \ldots, k_r$ secure up to

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

- 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 TEM Construction

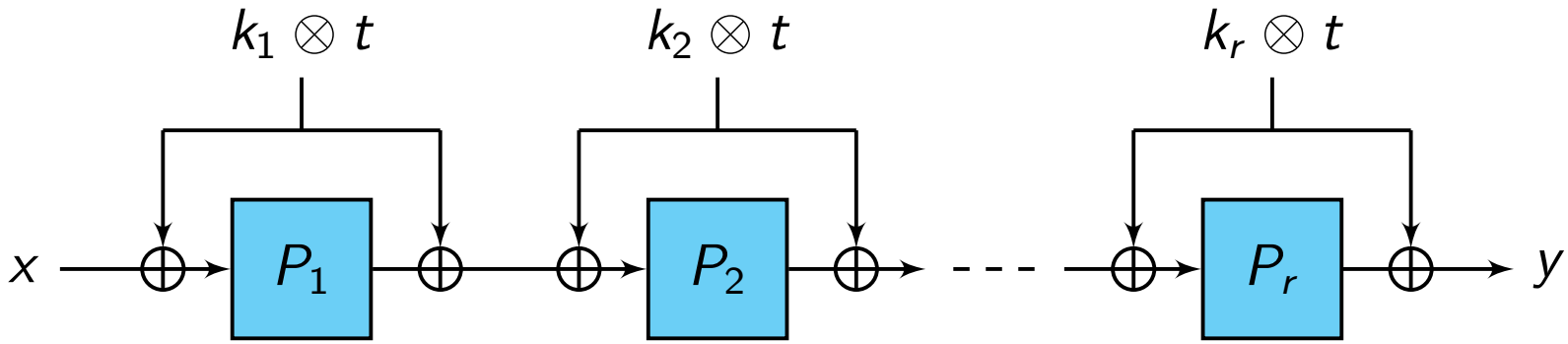


- r rounds, r even, with independent keys $k_1, \ldots, k_r$ secure up to

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

- 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 TEM Construction

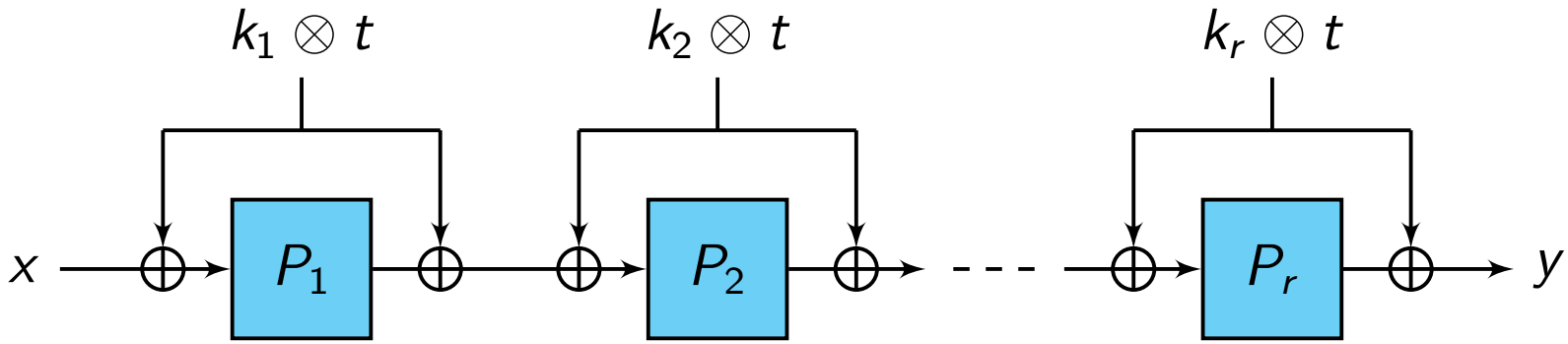


- r rounds, r even, with independent keys $k_1, \ldots, k_r$ secure up to

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

- 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 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

Outline

Background: Tweakable Block Ciphers

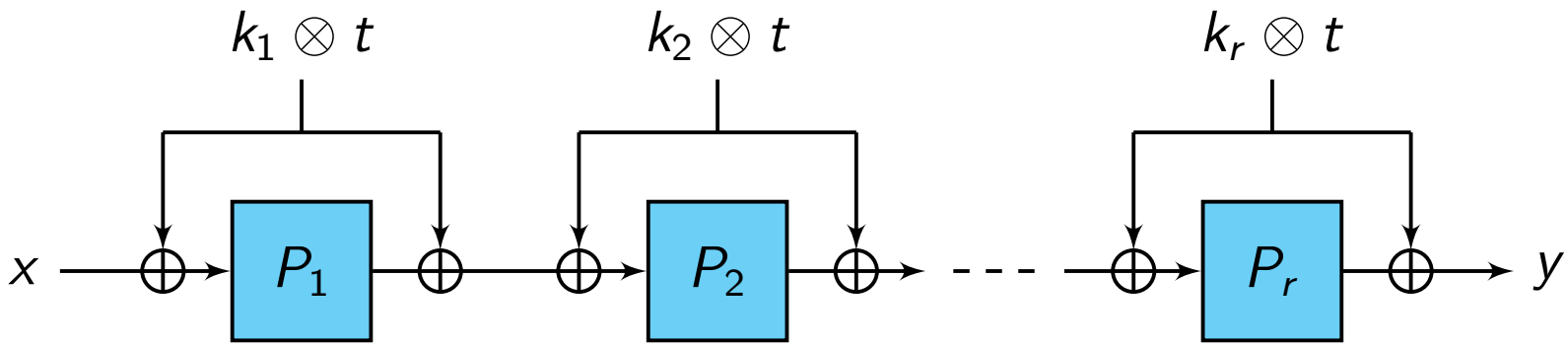
Our Contribution

Overview of the Proof for Two Rounds

Longer Cascades

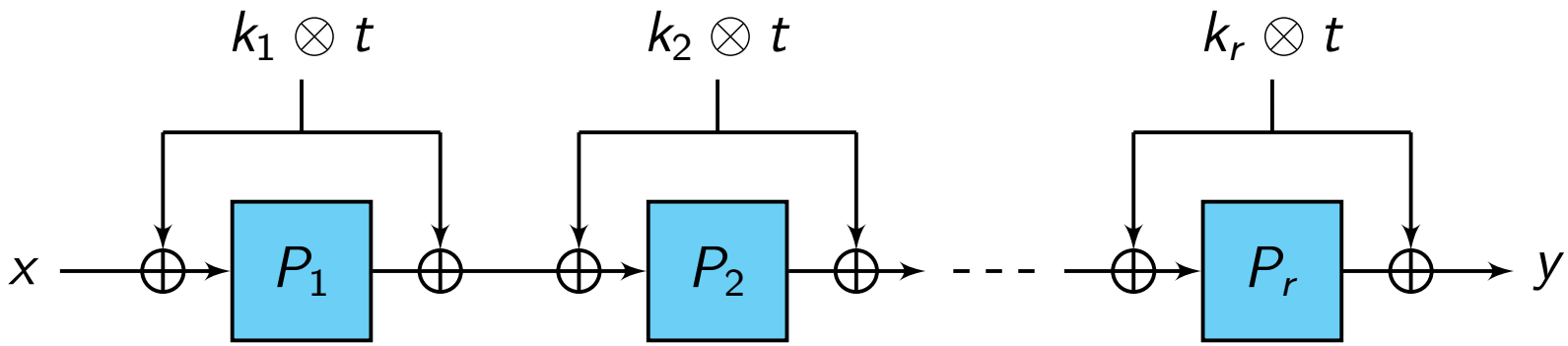
Conclusion and Perspectives

Conclusion



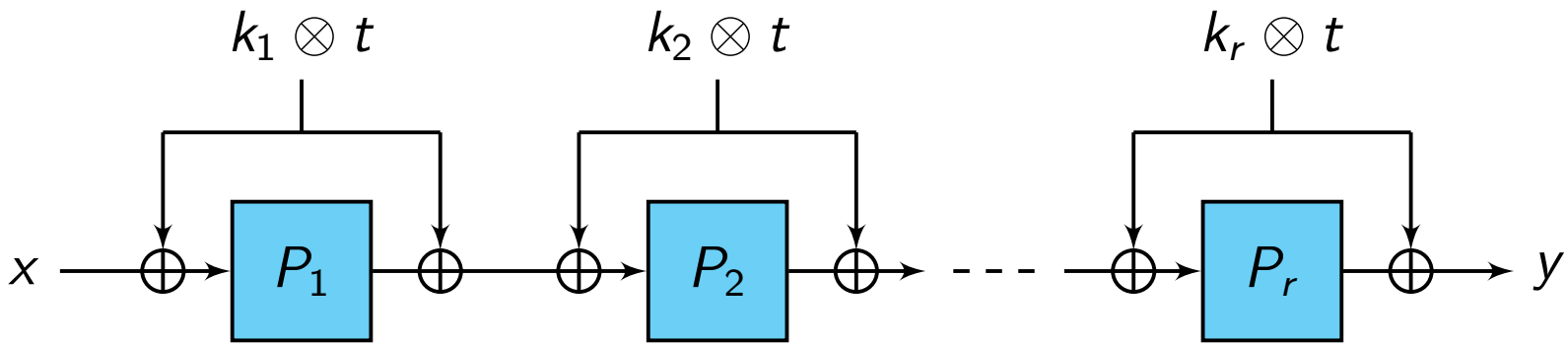
- we analyzed the "public permutation" variant of the LRW construction, and proved tight $2^{2n/3}$-security for 2 rounds
- similar security level as LRW, yet in an idealized model
- open problem 1: prove tight security up to $2^{\frac{rn}{r+1}}$ queries for $r \geq 3$
- open problem 2: can we avoid non-linear mixing of the key and the tweak and still get beyond-birthday security?

Conclusion



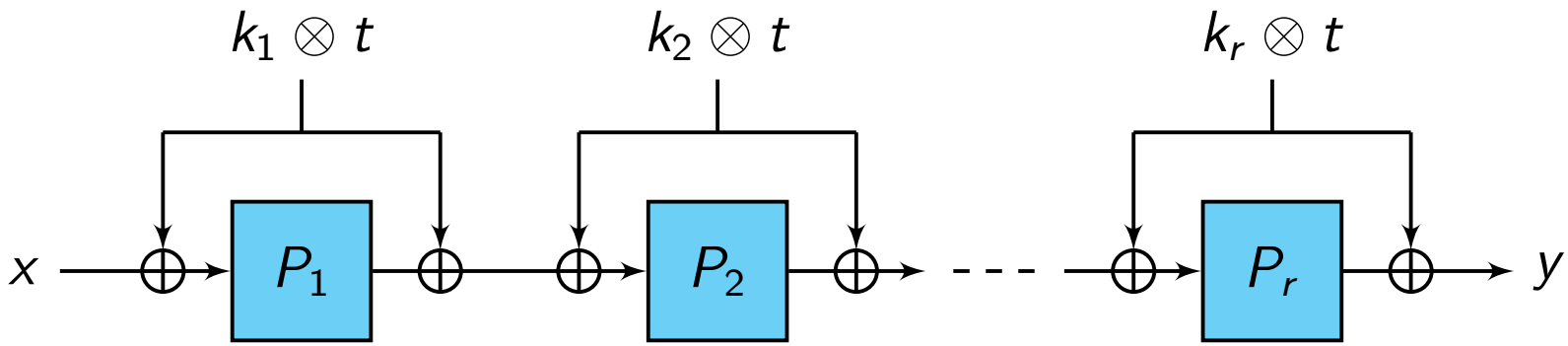
- we analyzed the "public permutation" variant of the LRW construction, and proved tight $2^{2n/3}$-security for 2 rounds
- similar security level as LRW, yet in an idealized model
- open problem 1: prove tight security up to $2^{\frac{rn}{r+1}}$ queries for $r \geq 3$
- open problem 2: can we avoid non-linear mixing of the key and the tweak and still get beyond-birthday security?

Conclusion



- we analyzed the "public permutation" variant of the LRW construction, and proved tight $2^{2n/3}$-security for 2 rounds
- similar security level as LRW, yet in an idealized model
- open problem 1: prove tight security up to $2^{\frac{rn}{r+1}}$ queries for $r \geq 3$
- open problem 2: can we avoid non-linear mixing of the key and the tweak and still get beyond-birthday security?

Conclusion



- we analyzed the "public permutation" variant of the LRW construction, and proved tight $2^{2n/3}$-security for 2 rounds
- similar security level as LRW, yet in an idealized model
- open problem 1: prove tight security up to $2^{\frac{rn}{r+1}}$ queries for $r \geq 3$
- open problem 2: can we avoid non-linear mixing of the key and the tweak and still get beyond-birthday security?

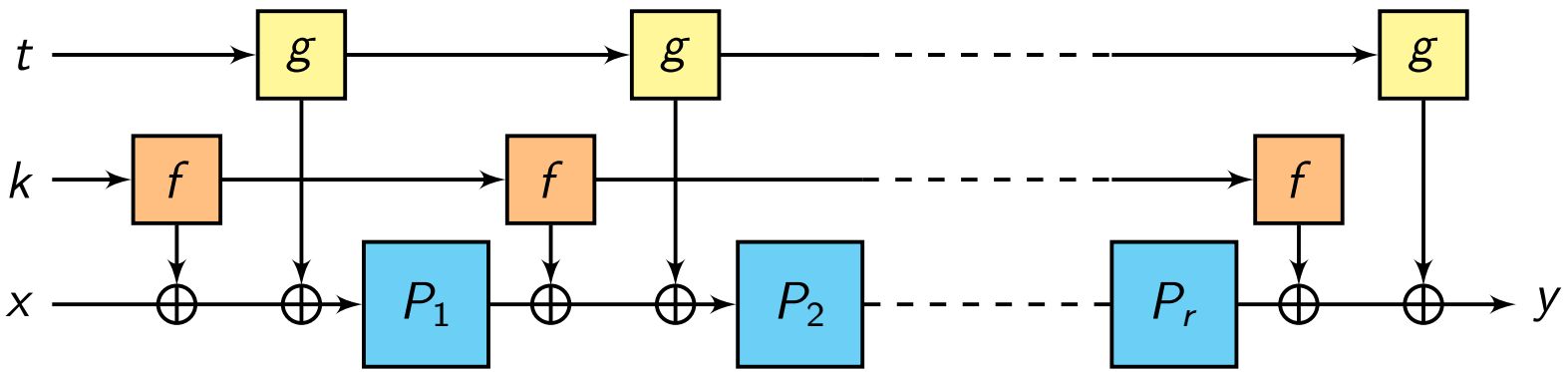
The TWEAKEY Framework

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

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

The TWEAKEY Framework

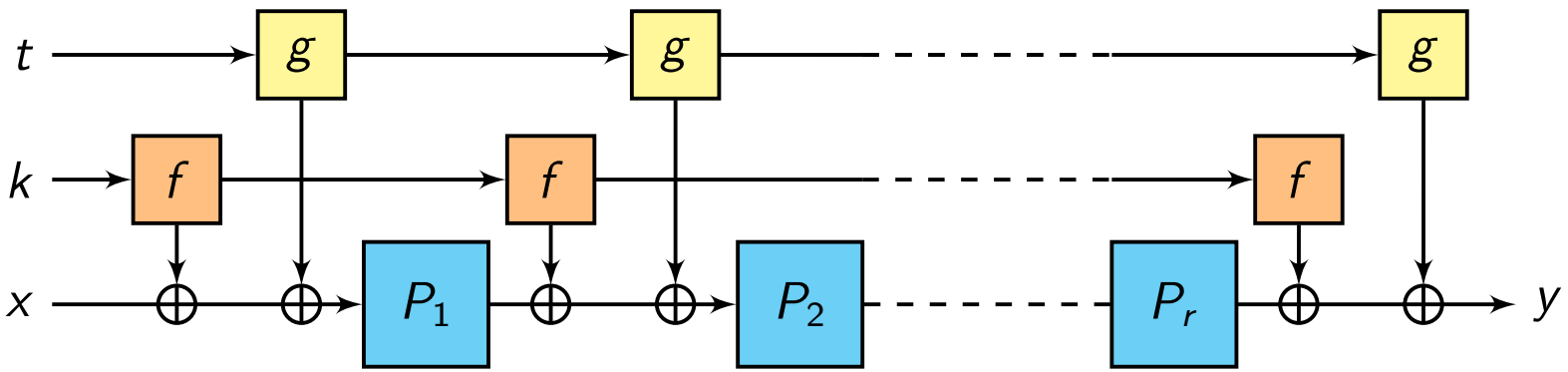
- proposed by Jean, Nikolić, and Peyrin [JNP14]
- Superposition TWEAKEY (STK) constructions:



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

The TWEAKEY Framework

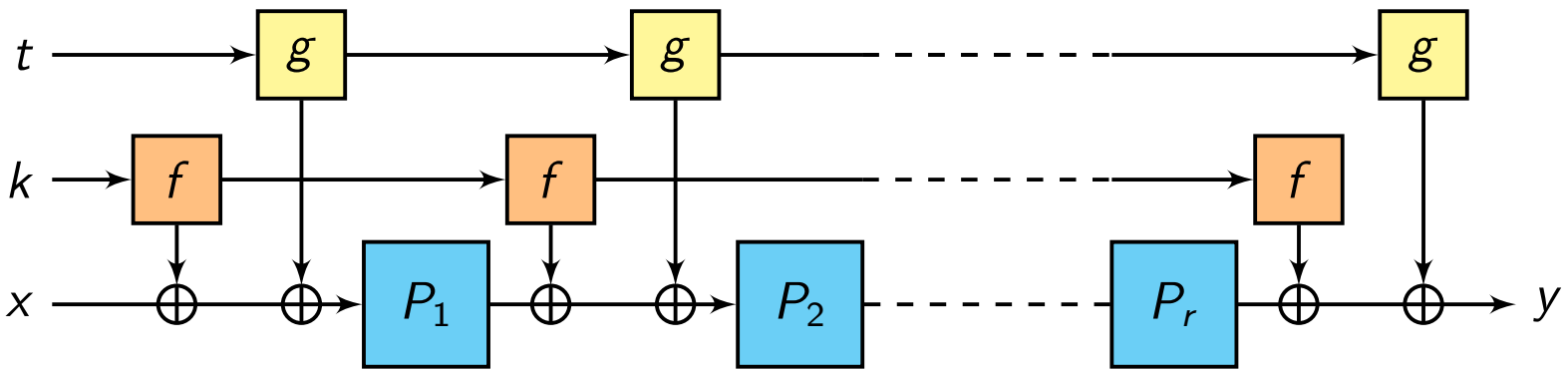
- proposed by Jean, Nikolić, and Peyrin [JNP14]
- Superposition TWEAKEY (STK) constructions:



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

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 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

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.

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

References II

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.

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.

References III


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`.


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.


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.