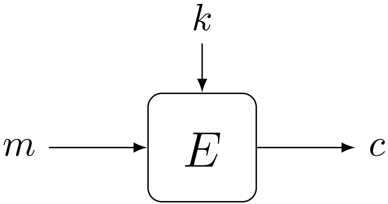
Towards Tight Security of Cascaded LRW2

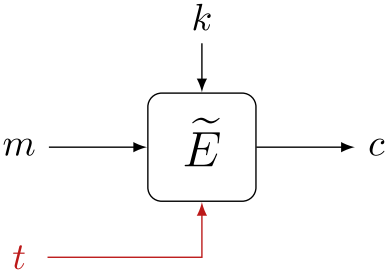
Bart Mennink
Radboud University (The Netherlands)

Theory of Cryptography Conference 2018
November 13, 2018

Tweakable Blockciphers

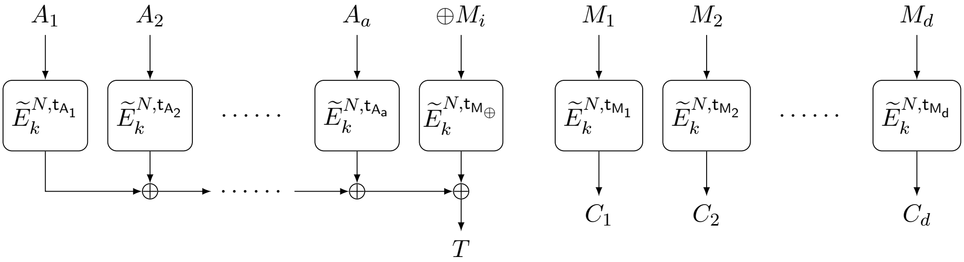


Tweakable Blockciphers



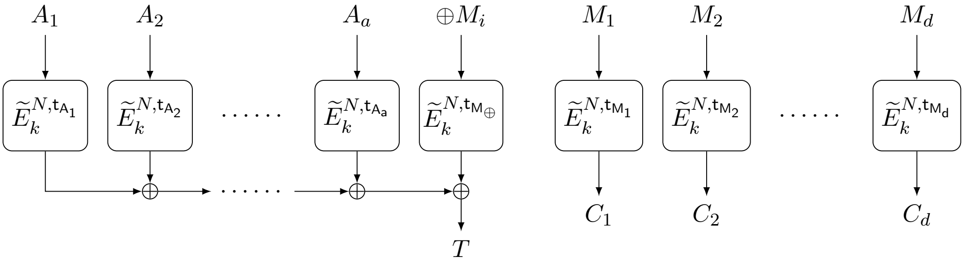
- Tweak: flexibility to the cipher
- Each tweak gives different permutation

Tweakable Blockciphers in OCBx



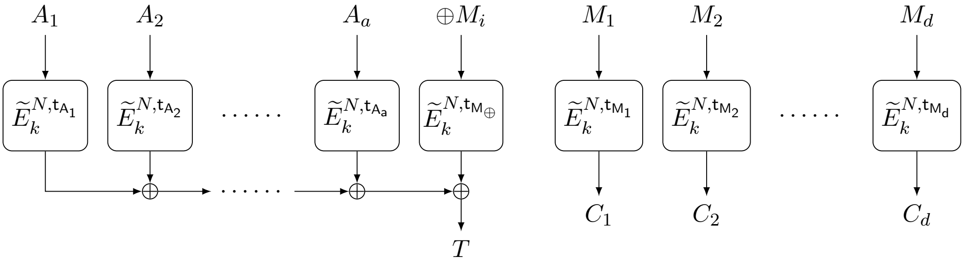
- Generalized OCB by Rogaway et al. [RBBK01,Rog04,KR11]

Tweakable Blockciphers in OCBx



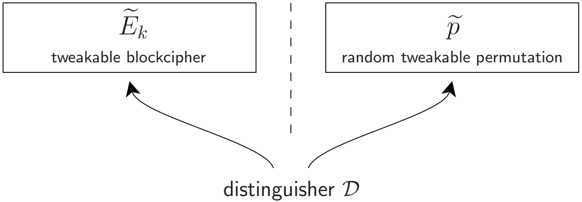
- Generalized OCB by Rogaway et al. [RBBK01,Rog04,KR11]
- Internally based on tweakable blockcipher $\widetilde{E}$
  - Tweak (N, index) is unique for every evaluation
  - Different blocks always transformed under different tweak

Tweakable Blockciphers in OCBx



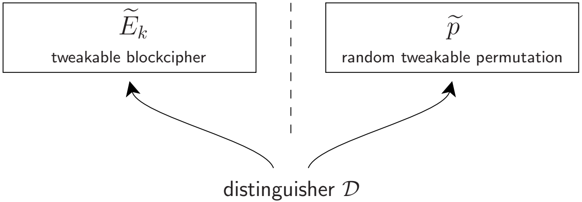
- Generalized OCB by Rogaway et al. [RBBK01,Rog04,KR11]
- Internally based on tweakable blockcipher $\widetilde{E}$
  - Tweak (N, index) is unique for every evaluation
  - Different blocks always transformed under different tweak
- Security of mode often dictated by that of $\widetilde{E}$

Tweakable Blockcipher Security



- $\widetilde{E}_k$ should look like random permutation for every t
- Different tweaks $\longrightarrow$ pseudo-independent permutations

Tweakable Blockcipher Security

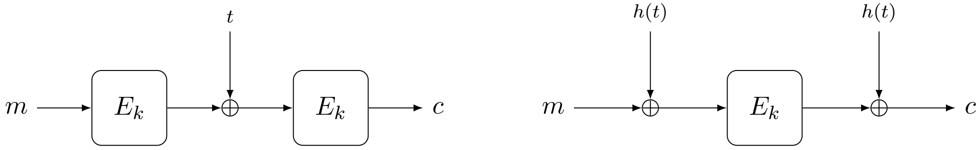


- $\widetilde{E}_k$ should look like random permutation for every t
- Different tweaks $\longrightarrow$ pseudo-independent permutations
- $\mathcal{D}$ tries to determine which oracle it communicates with

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{stprp}}(\mathcal{D}) = \left|\mathbf{Pr}\left[\mathcal{D}^{\widetilde{E}_k,\widetilde{E}_k^{-1}} = 1\right] - \mathbf{Pr}\left[\mathcal{D}^{\widetilde{\pi},\widetilde{\pi}^{-1}} = 1\right]\right|$$

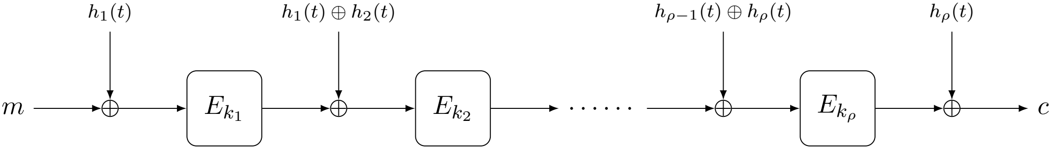
Original Constructions

- LRW_1 and LRW_2 by Liskov et al. [LRW02]:



- h is XOR-universal hash
- Related: XEX [Rog04] and relatives
- Tightly secure up to $2^{n/2}$ queries

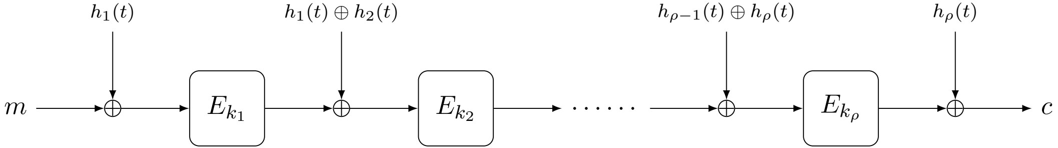
Cascading LRW_2's



- $\mathsf{LRW}_2[\rho]$: concatenation of ρ LRW_2's
- $k_1, \ldots, k_\rho$ and $h_1, \ldots, h_\rho$ independent

"Cascaded LRW_2"
$= \mathsf{LRW}_2[2]$

Cascading LRW_2's

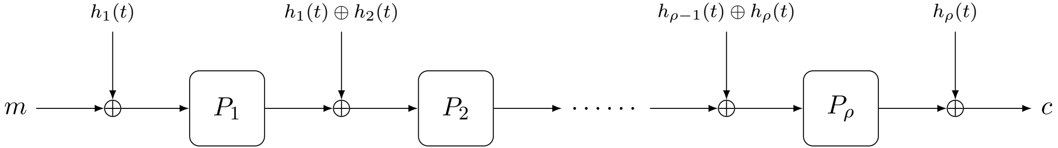


- $\mathsf{LRW}_2[\rho]$: concatenation of ρ LRW_2's
- $k_1, \ldots, k_\rho$ and $h_1, \ldots, h_\rho$ independent

"Cascaded LRW_2" $= \mathsf{LRW}_2[2]$

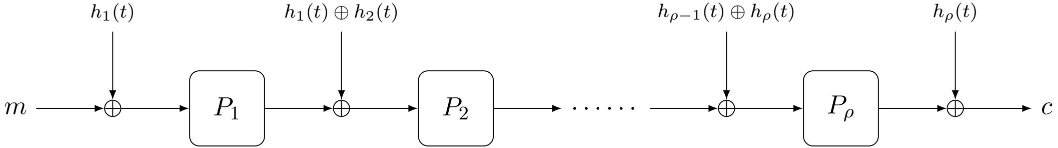
- $\rho = 2$: secure up to $2^{2n/3}$ queries [LST12,Pro14]
- $\rho \geq 2$ even: secure up to $2^{\rho n/(\rho+2)}$ queries [LS13]
- Best attack: 2^n queries

Cascading TEM's



- TEM[ρ]: concatenation of ρ TEM's
- $P_1, \ldots, P_\rho$ and $h_1, \ldots, h_\rho$ independent

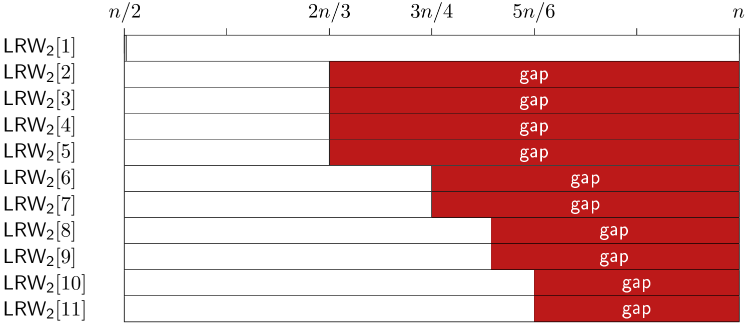
Cascading TEM's

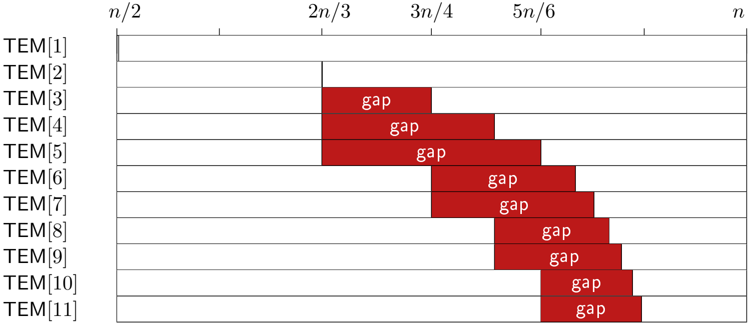


- TEM$[\rho]$: concatenation of ρ TEM's
- $P_1, \ldots, P_\rho$ and $h_1, \ldots, h_\rho$ independent

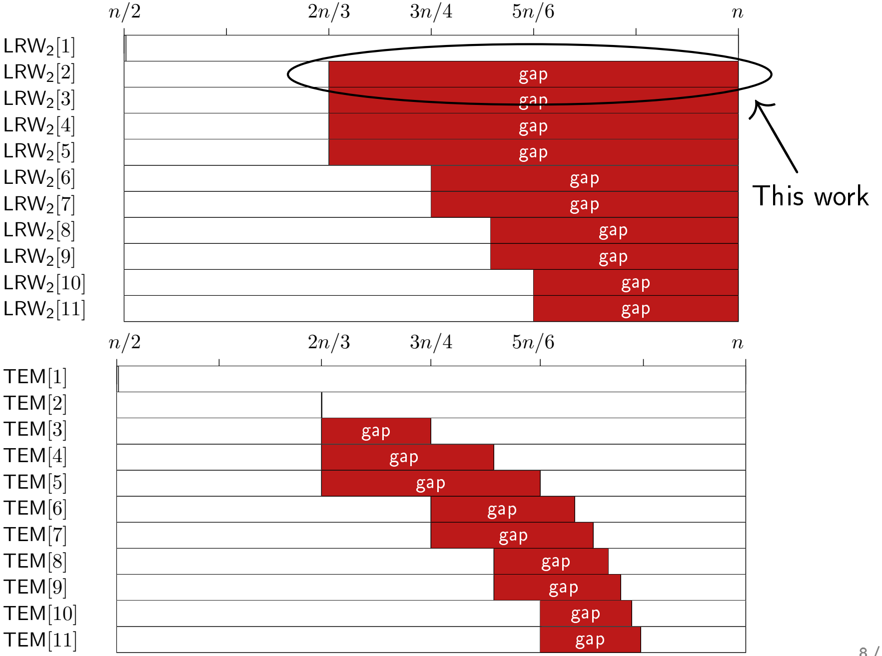
- $\rho = 2$: secure up to $2^{2n/3}$ queries [CLS15]
- $\rho \geq 2$ even: secure up to $2^{\rho n/(\rho+2)}$ queries [CLS15]
- Best attack: $2^{\rho n/(\rho+1)}$ queries [BKL+12]

State of the Art

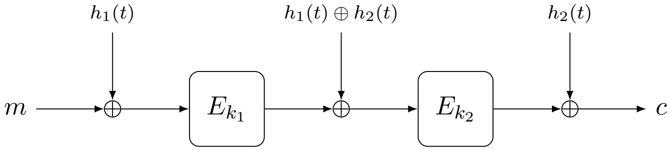


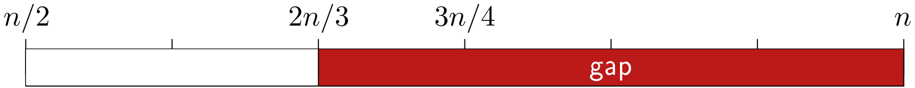


State of the Art

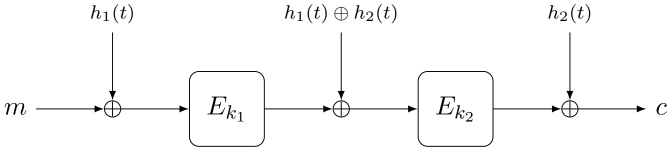


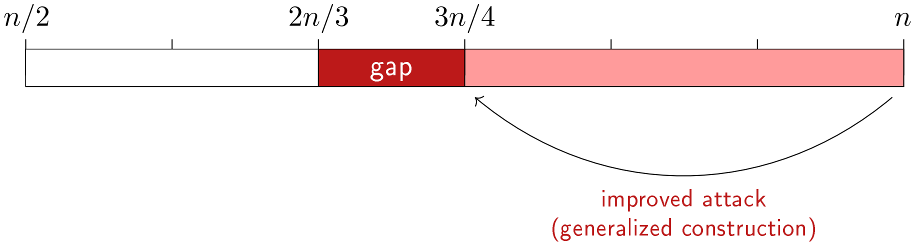
Tight Security of Cascaded LRW$_2$?



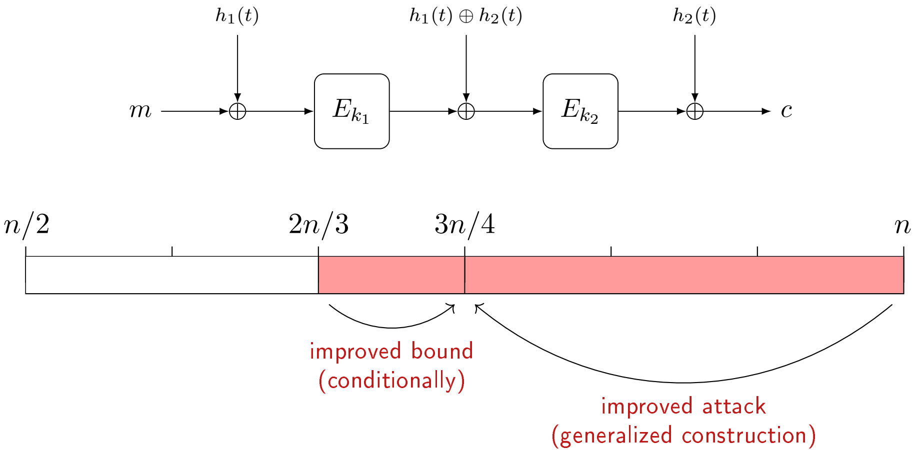


Tight Security of Cascaded LRW_2?

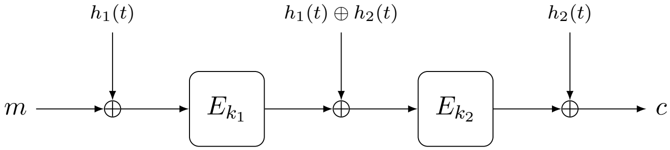


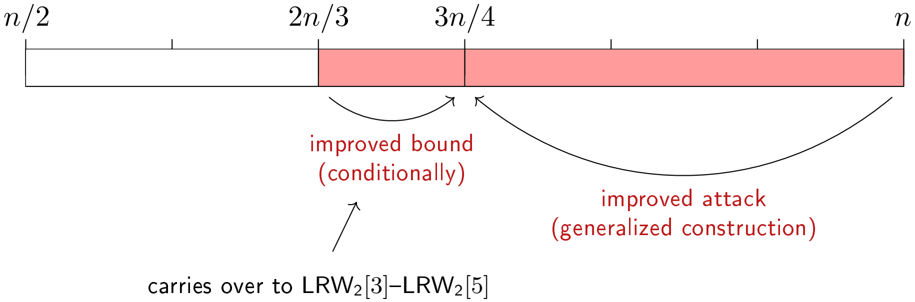


Tight Security of Cascaded LRW_2?



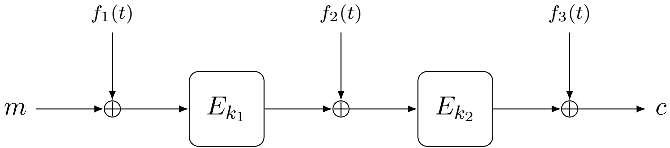
Tight Security of Cascaded LRW_2?





Improved Attack

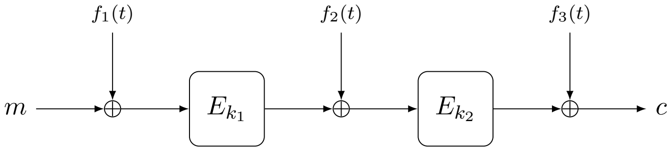
- GCL (Generalized Cascaded LRW_2):



- f_i are arbitrary functions
- $p_i := E_{k_i}$ are random permutations

Improved Attack

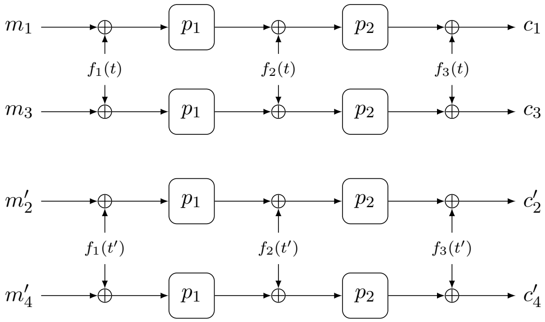
- GCL (Generalized Cascaded LRW$_2$):



- f_i are arbitrary functions
- $p_i := E_{k_i}$ are random permutations

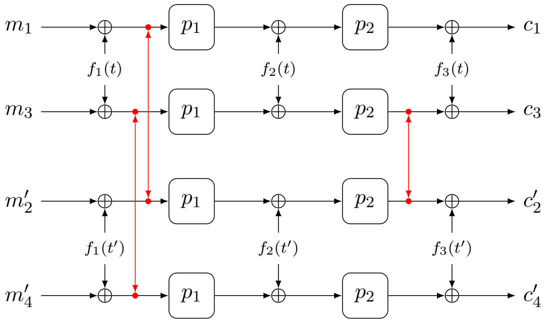
Generic distinguishing attack in $2n^{1/2}2^{3n/4}$ evaluations

Improved Attack: Rationale



- Distinguisher $\mathcal{D}$ makes various queries for two different tweaks: t and t'

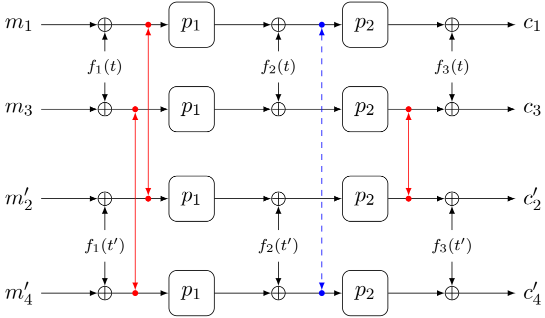
Improved Attack: Rationale



- Distinguisher $\mathcal{D}$ makes various queries for two different tweaks: t and t'
- Suppose it makes 4 queries such that

$$m_1 \oplus f_1(t) = m'_2 \oplus f_1(t')$$
$$c'_2 \oplus f_3(t') = c_3 \oplus f_3(t)$$
$$m_3 \oplus f_1(t) = m'_4 \oplus f_1(t')$$

Improved Attack: Rationale



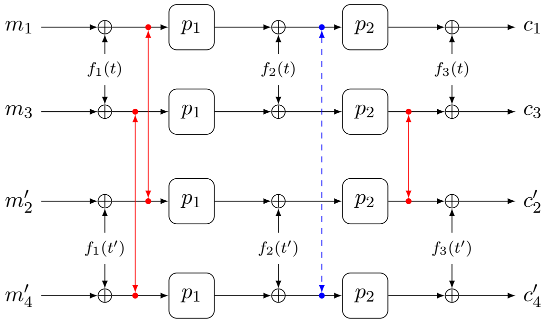
- Distinguisher $\mathcal{D}$ makes various queries for two different tweaks: t and t'
- Suppose it makes 4 queries such that

$$m_1 \oplus f_1(t) = m_2' \oplus f_1(t')$$
$$c_2' \oplus f_3(t') = c_3 \oplus f_3(t)$$
$$m_3 \oplus f_1(t) = m_4' \oplus f_1(t')$$

- Necessarily,

$$c_1 \oplus f_3(t) = c_4' \oplus f_3(t')$$

Improved Attack: Rationale



- Distinguisher $\mathcal{D}$ makes various queries for two different tweaks: t and t'
- Suppose it makes 4 queries such that

$$m_1 \oplus f_1(t) = m'_2 \oplus f_1(t')$$
$$c'_2 \oplus f_3(t') = c_3 \oplus f_3(t)$$
$$m_3 \oplus f_1(t) = m'_4 \oplus f_1(t')$$

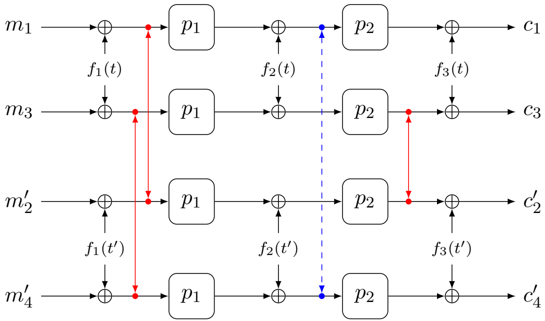
- Necessarily,

$$c_1 \oplus f_3(t) = c'_4 \oplus f_3(t')$$

- Stated differently:

$$m_1 \oplus m'_2 = m_3 \oplus m'_4 = f_1(t) \oplus f_1(t')$$
$$c'_2 \oplus c_3 = c_1 \oplus c'_4 = f_3(t) \oplus f_3(t')$$

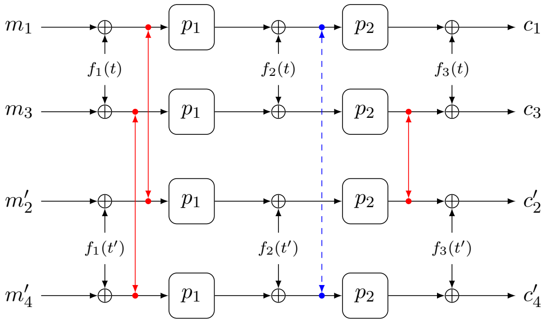
Improved Attack: Rationale



- Stated differently:

$$m_1 \oplus m_2' = m_3 \oplus m_4' = f_1(t) \oplus f_1(t')$$
$$c_2' \oplus c_3 = c_1 \oplus c_4' = f_3(t) \oplus f_3(t')$$

Improved Attack: Rationale

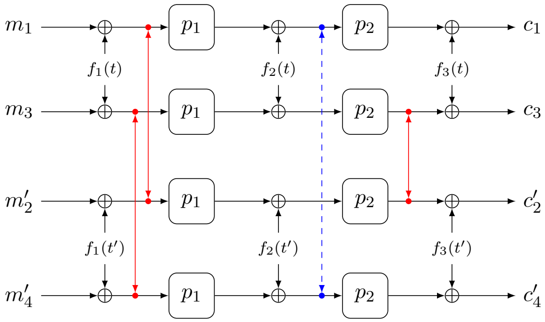


- Stated differently:

$$m_1 \oplus m_2' = m_3 \oplus m_4' = f_1(t) \oplus f_1(t')$$
$$c_2' \oplus c_3 = c_1 \oplus c_4' = f_3(t) \oplus f_3(t')$$

- But $\mathcal{D}$ does not know $f_1(t) \oplus f_1(t')$

Improved Attack: Rationale

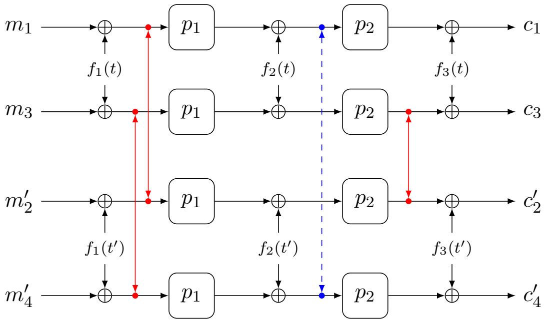


- Stated differently:

  $$m_1 \oplus m_2' = m_3 \oplus m_4' = f_1(t) \oplus f_1(t')$$
  $$c_2' \oplus c_3 = c_1 \oplus c_4' = f_3(t) \oplus f_3(t')$$

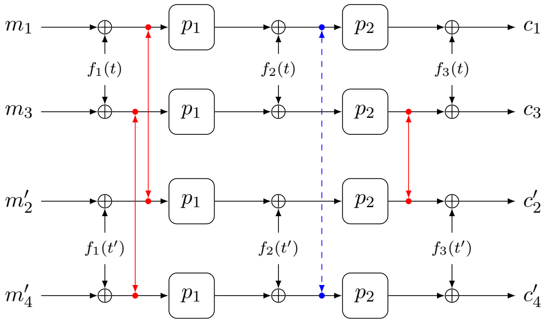
- But $\mathcal{D}$ does not know $f_1(t) \oplus f_1(t')$
- Choose the m_i's and m_i''s such that for any d, there are 2^n quadruples such that $m_1 \oplus m_2' = m_3 \oplus m_4' = d$ (costs $2^{3n/4}$ queries for both t and t')

Improved Attack: Rationale



- Stated differently:
  $$m_1 \oplus m'_2 = m_3 \oplus m'_4 = f_1(t) \oplus f_1(t')$$
  $$c'_2 \oplus c_3 = c_1 \oplus c'_4 = f_3(t) \oplus f_3(t')$$
- But $\mathcal{D}$ does not know $f_1(t) \oplus f_1(t')$
- Choose the m_i's and m'_i's such that for any d, there are 2^n quadruples such that $m_1 \oplus m'_2 = m_3 \oplus m'_4 = d$ (costs $2^{3n/4}$ queries for both t and t')
- $\mathbb{E}$[solutions to $c'_2 \oplus c_3 = c_1 \oplus c'_4$]?
  2 if $d = f_1(t) \oplus f_1(t')$, 1 otherwise

Improved Attack: Rationale



- Stated differently:

$$m_1 \oplus m'_2 = m_3 \oplus m'_4 = f_1(t) \oplus f_1(t')$$
$$c'_2 \oplus c_3 = c_1 \oplus c'_4 = f_3(t) \oplus f_3(t')$$

- But $\mathcal{D}$ does not know $f_1(t) \oplus f_1(t')$
- Choose the m_i's and m'_i's such that for any d, there are 2^n quadruples such that $m_1 \oplus m'_2 = m_3 \oplus m'_4 = d$ (costs $2^{3n/4}$ queries for both t and t')
- $\mathbb{E}$[solutions to $c'_2 \oplus c_3 = c_1 \oplus c'_4$]? 2 if $d = f_1(t) \oplus f_1(t')$, 1 otherwise
- Extend the number of queries by factor $n^{1/2}$ to eliminate false positives

Improved Attack: Verification

Theoretical Verification

- Assuming $n \geq 27$, the success probability of $\mathcal{D}$ is at least $1/2$
- Analysis consists of properly bounding $\mathbf{Pr}\left[\mathcal{D}^{\widetilde{E}_k} = 1\right]$ and $\mathbf{Pr}\left[\mathcal{D}^{\widetilde{\pi}} = 1\right]$

Improved Attack: Verification

Theoretical Verification

- Assuming $n \geq 27$, the success probability of $\mathcal{D}$ is at least $1/2$
- Analysis consists of properly bounding $\mathbf{Pr}\left[\mathcal{D}^{\widetilde{E}_k} = 1\right]$ and $\mathbf{Pr}\left[\mathcal{D}^{\widetilde{\pi}} = 1\right]$

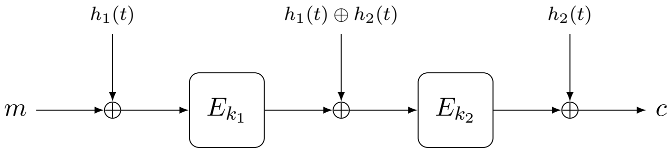
Experimental Verification

- Small-scale implementation for $n = 16, 20, 24$
- N_d is the number of hits $c_2' \oplus c_3 = c_1 \oplus c_4'$

			N_d in real world for $d =$		N_d in ideal world for $d =$	
n	$n^{1/2} \approx$	q	$f_1(t) \oplus f_1(t')$	random	$f_1(t) \oplus f_1(t')$	random
16	2	$4 \cdot 2^{12}$	256.593750	129.781250	127.093750	127.375000
20	2	$4 \cdot 2^{15}$	265.531250	133.312500	125.625000	128.750000
24	2	$4 \cdot 2^{18}$	246.750000	131.375000	120.625000	129.875000

Improved Security Bound

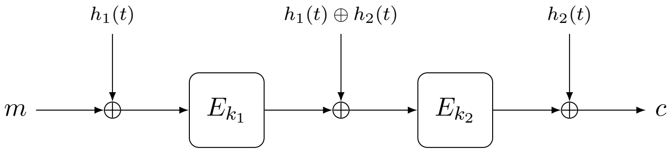
- Cascaded LRW_2:



- E_{k_i} are SPRP-secure
- h_i are 4-wise independent XOR-universal hash
- No tweak is queried more than $2^{n/4}$ times

Improved Security Bound

- Cascaded LRW_2:



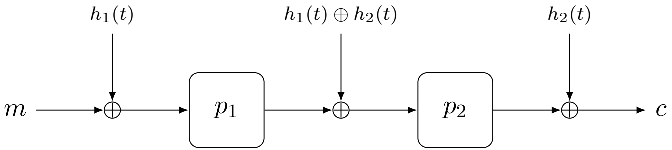
- E_{k_i} are SPRP-secure
- h_i are 4-wise independent XOR-universal hash
- No tweak is queried more than $2^{n/4}$ times

Cascaded LRW_2 is secure up to $\approx 2^{3n/4}$ evaluations

Improved Security Bound: Proof Idea (1)

Step 1: SPRP Switch

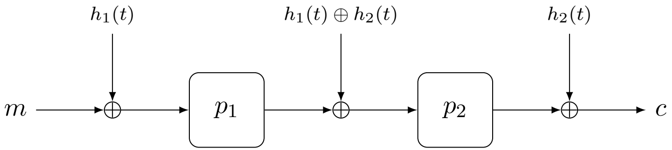
- Replace E_{k_i} by random permutations p_i



Improved Security Bound: Proof Idea (1)

Step 1: SPRP Switch

- Replace E_{k_i} by random permutations p_i

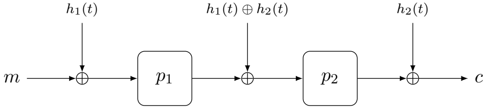


Step 2: Patarin's H-Coefficient Technique

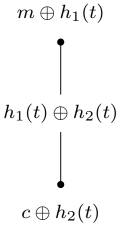
- Main task: given q evaluations of cascaded LRW_2, derive lower bound on $\#\{(p_1, p_2)\}$
- Lower bound should hold for the "most likely" transcripts

Improved Security Bound: Proof Idea (2)

Step 3: Transform Transcript to Graph (One Tuple)

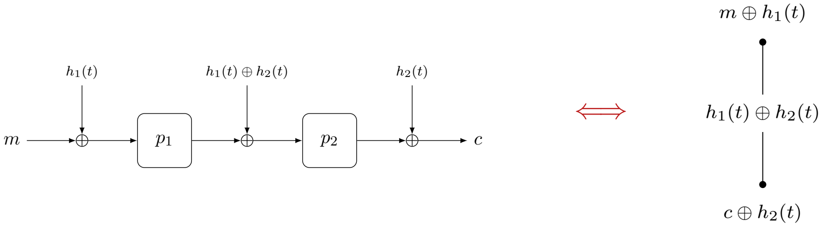


$\Longleftrightarrow$



Improved Security Bound: Proof Idea (2)

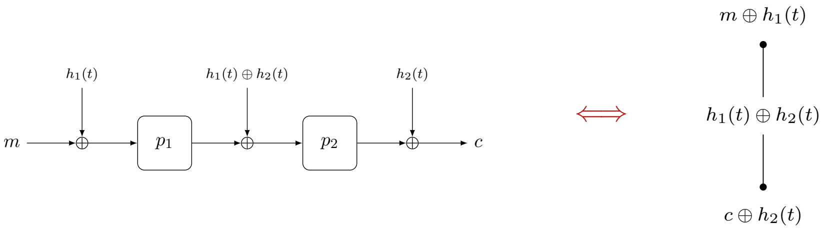
Step 3: Transform Transcript to Graph (One Tuple)



- 2 unknowns: $X := p_1(m \oplus h_1(t))$ and $Y := p_2^{-1}(c \oplus h_2(t))$
- 1 equation: $X \oplus Y = h_1(t) \oplus h_2(t)$

Improved Security Bound: Proof Idea (2)

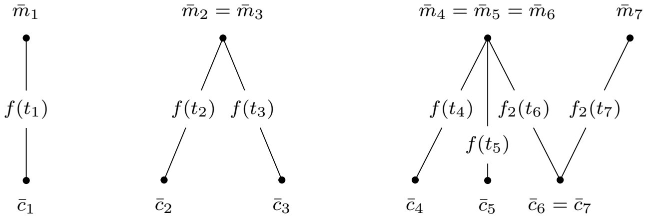
Step 3: Transform Transcript to Graph (One Tuple)



- 2 unknowns: $X := p_1(m \oplus h_1(t))$ and $Y := p_2^{-1}(c \oplus h_2(t))$
- 1 equation: $X \oplus Y = h_1(t) \oplus h_2(t)$
- Lower bound on $\#\{(p_1, p_2)\}$ related to the number of choices (X, Y)

Improved Security Bound: Proof Idea (3)

Step 4: Transform Transcript to Graph (All Tuples)



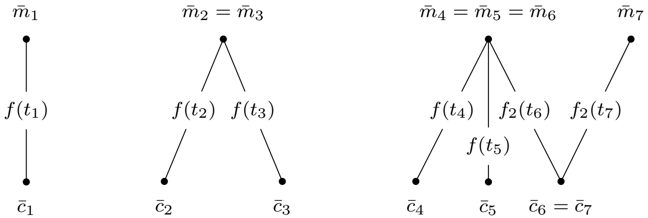
notation:

$$\bar{m}_i = m_i \oplus h_1(t_i)$$
$$\bar{c}_i = c_i \oplus h_2(t_i)$$
$$f(t_i) = h_1(t_i) \oplus h_2(t_i)$$

- r_1 unknowns for p_1, r_2 unknowns for p_2, and q equations

Improved Security Bound: Proof Idea (3)

Step 4: Transform Transcript to Graph (All Tuples)



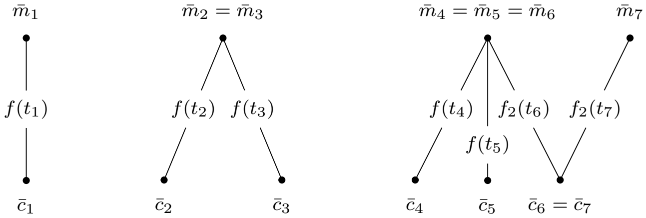
notation:

$$\bar{m}_i = m_i \oplus h_1(t_i)$$
$$\bar{c}_i = c_i \oplus h_2(t_i)$$
$$f(t_i) = h_1(t_i) \oplus h_2(t_i)$$

- r_1 unknowns for p_1, r_2 unknowns for p_2, and q equations
- Two potential problems:
  - (i) Graph contains circle
  - (ii) Graph contains path of even length whose labels sum to 0 (degeneracy)

Improved Security Bound: Proof Idea (3)

Step 4: Transform Transcript to Graph (All Tuples)



notation:

$$\bar{m}_i = m_i \oplus h_1(t_i)$$
$$\bar{c}_i = c_i \oplus h_2(t_i)$$
$$f(t_i) = h_1(t_i) \oplus h_2(t_i)$$

- r_1 unknowns for p_1, r_2 unknowns for p_2, and q equations
- Two potential problems:
  - (i) Graph contains circle
  - (ii) Graph contains path of even length whose labels sum to 0 (degeneracy)
- If neither of these occurs: one "free choice" for each tree

Improved Security Bound: Proof Idea (4)

Step 5: Patarin's Mirror Theory (Informal)

If the graph is (i) circle free, (ii) non-degenerate, and (iii) has no excessively large tree, the number of possible (p_1, p_2) is at least

$$\frac{2^n!2^n!}{2^{nq}} \cdot \left(1 - \frac{4q}{2^n}\right)$$

Improved Security Bound: Proof Idea (4)

Step 5: Patarin's Mirror Theory (Informal)

If the graph is (i) circle free, (ii) non-degenerate, and (iii) has no excessively large tree, the number of possible (p_1, p_2) is at least

$$\frac{2^n!2^n!}{2^{nq}} \cdot \left(1 - \frac{4q}{2^n}\right)$$

- Lower bound on $\#\{(p_1, p_2)\}$ sufficient to derive $2^{3n/4}$ security (some technicality involved)
- Violation of (i), (ii), or (iii) with probability at most $O(q^4/2^{3n})$

Improved Security Bound: Proof Idea (4)

Step 5: Patarin's Mirror Theory (Informal)

If the graph is (i) circle free, (ii) non-degenerate, and (iii) has no excessively large tree, the number of possible (p_1, p_2) is at least

$$\frac{2^n! 2^n!}{2^{nq}} \cdot \left(1 - \frac{4q}{2^n}\right)$$

- Lower bound on $\#\{(p_1, p_2)\}$ sufficient to derive $2^{3n/4}$ security (some technicality involved)
- Violation of (i), (ii), or (iii) with probability at most $O(q^4/2^{3n})$
- We apply mirror theory up to the first iteration

Improved Security Bound: Bottlenecks

Excessively Large Tree

- Badness probability relies on
  - tweak limitation
  - 4-wise independence of hash functions

Mirror Theory

- Mirror theory developed for comparison with PRF, not with PRP
- Problem mitigated due to tweak limitation

Conclusion

Cascaded LRW_2 (or $\mathsf{LRW}_2[2]$)

- Generic attack in complexity $3n/4$
- $3n/4$ security bound, but conditional
- Security bound carries over to $\mathsf{LRW}_2[3]$–$\mathsf{LRW}_2[5]$

Conclusion

Cascaded LRW_2 (or $LRW_2[2]$)

- Generic attack in complexity $3n/4$
- $3n/4$ security bound, but conditional
- Security bound carries over to $LRW_2[3]$–$LRW_2[5]$

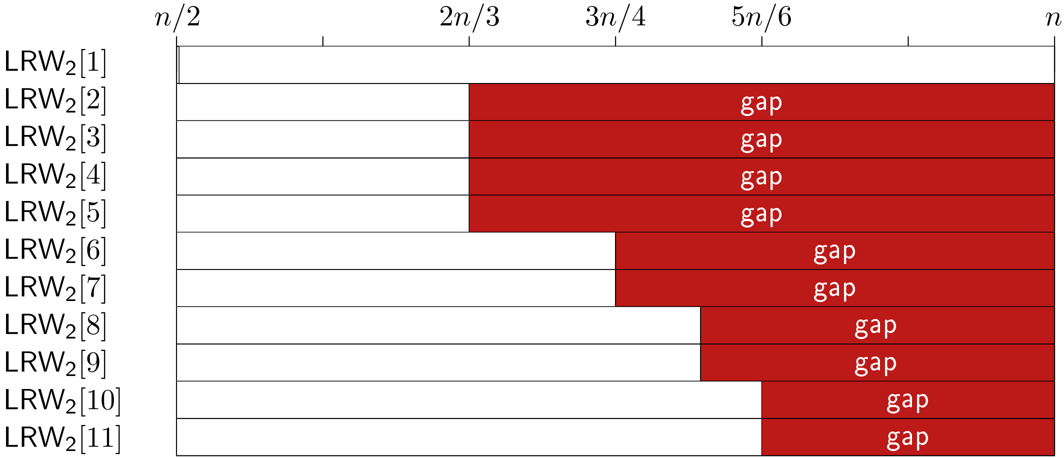
Challenges

- Tightness of cascaded LRW_2 without side conditions?
- Longer cascades of $LRW_2[\rho]$ and $TEM[\rho]$?

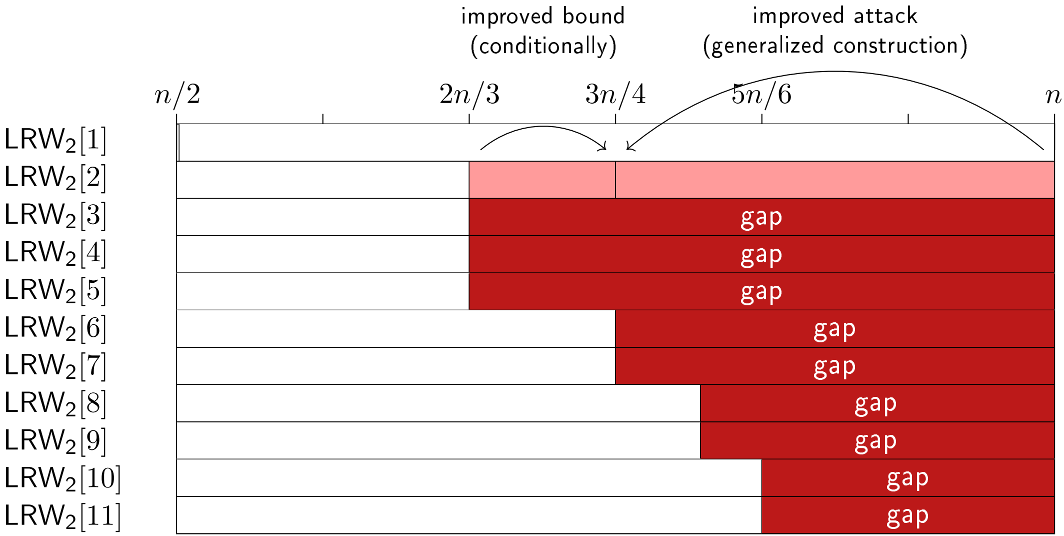
Thank you for your attention!

SUPPORTING SLIDES

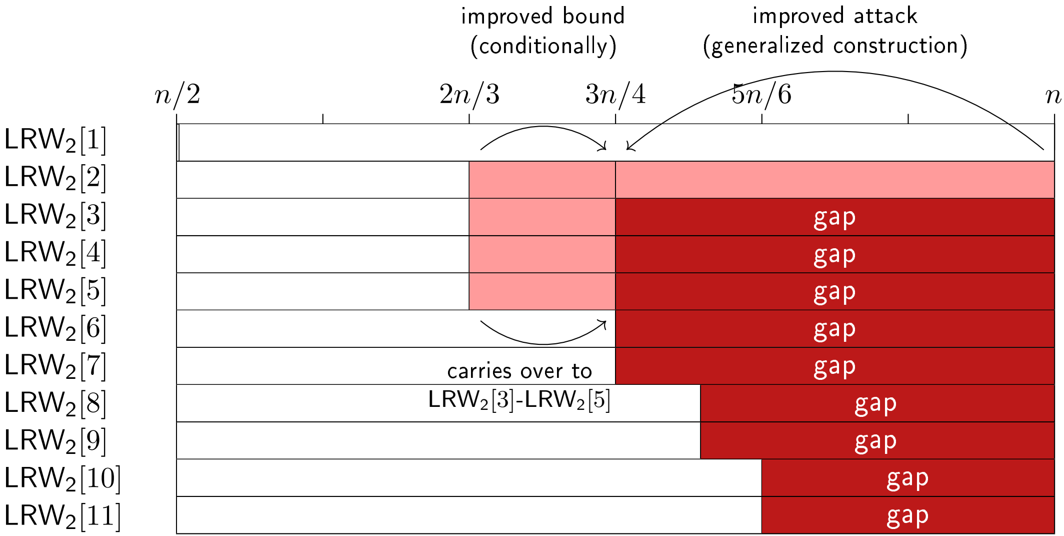
Updated State of the Art on $\mathsf{LRW}_2[\rho]$



Updated State of the Art on $LRW_2[\rho]$



Updated State of the Art on $\mathsf{LRW}_2[\rho]$

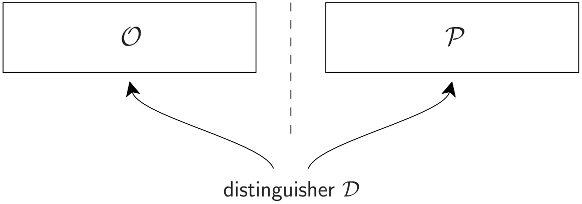


H-Coefficient Technique

- Patarin [Pat91,Pat08]
- Popularized by Chen and Steinberger [CS14]
- Similar to “Strong Interpolation Technique” [Ber05]

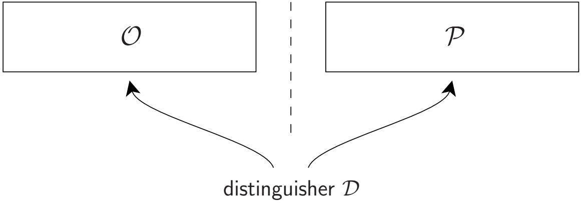
H-Coefficient Technique

- Patarin [Pat91,Pat08]
- Popularized by Chen and Steinberger [CS14]
- Similar to "Strong Interpolation Technique" [Ber05]



H-Coefficient Technique

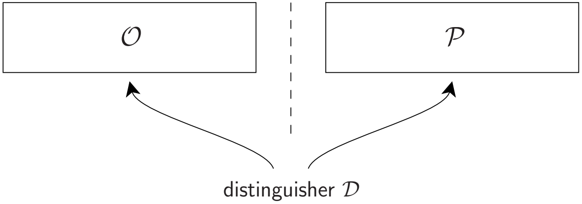
- Patarin [Pat91,Pat08]
- Popularized by Chen and Steinberger [CS14]
- Similar to "Strong Interpolation Technique" [Ber05]



- Basic idea:
  - Each conversation defines a transcript τ

H-Coefficient Technique

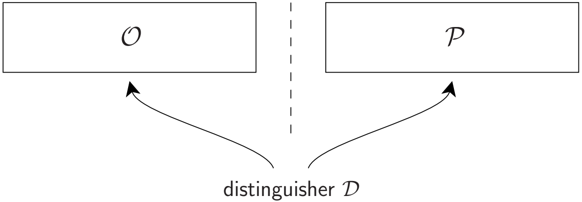
- Patarin [Pat91,Pat08]
- Popularized by Chen and Steinberger [CS14]
- Similar to "Strong Interpolation Technique" [Ber05]



- Basic idea:
  - Each conversation defines a transcript τ
  - $\mathcal{O} \approx \mathcal{P}$ for most of the transcripts

H-Coefficient Technique

- Patarin [Pat91,Pat08]
- Popularized by Chen and Steinberger [CS14]
- Similar to "Strong Interpolation Technique" [Ber05]



- Basic idea:
  - Each conversation defines a transcript τ
  - $\mathcal{O} \approx \mathcal{P}$ for most of the transcripts
  - Remaining transcripts occur with small probability

H-Coefficient Technique

- $\mathcal{D}$ is computationally unbounded and deterministic
- Each conversation defines a transcript τ

H-Coefficient Technique

- $\mathcal{D}$ is computationally unbounded and deterministic
- Each conversation defines a transcript τ
- Consider good and bad transcripts

H-Coefficient Technique

- $\mathcal{D}$ is computationally unbounded and deterministic
- Each conversation defines a transcript τ
- Consider good and bad transcripts

Lemma

Let $\varepsilon \geq 0$ be such that for all good transcripts τ:

$$\frac{\mathbf{Pr}\left[\mathcal{O} \text{ gives } \tau\right]}{\mathbf{Pr}\left[\mathcal{P} \text{ gives } \tau\right]} \geq 1 - \varepsilon$$

Then, $\Delta_{\mathcal{D}}(\mathcal{O}; P) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } \mathcal{P}\right]$

H-Coefficient Technique

- $\mathcal{D}$ is computationally unbounded and deterministic
- Each conversation defines a transcript τ
- Consider good and bad transcripts

Lemma

Let $\varepsilon \geq 0$ be such that for all good transcripts τ:

$$\frac{\mathbf{Pr}\left[\mathcal{O} \text{ gives } \tau\right]}{\mathbf{Pr}\left[\mathcal{P} \text{ gives } \tau\right]} \geq 1 - \varepsilon$$

Then, $\Delta_{\mathcal{D}}(\mathcal{O}; P) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } \mathcal{P}\right]$

Trade-off: define bad transcripts smartly!

Mirror Theory

System of Equations

- Consider r distinct unknowns $\mathcal{P} = \{P_1, \ldots, P_r\}$
- Consider a system of q equations of the form:

$$
\begin{aligned}
P_{a_1} \oplus P_{b_1} &= \lambda_1 \\
P_{a_2} \oplus P_{b_2} &= \lambda_2 \\
&\vdots \\
P_{a_q} \oplus P_{b_q} &= \lambda_q
\end{aligned}
$$

for some surjection $\varphi : \{a_1, b_1, \ldots, a_q, b_q\} \to \{1, \ldots, r\}$

Mirror Theory

System of Equations

- Consider r distinct unknowns $\mathcal{P} = \{P_1, \ldots, P_r\}$
- Consider a system of q equations of the form:

$$\begin{aligned} P_{a_1} \oplus P_{b_1} &= \lambda_1 \\ P_{a_2} \oplus P_{b_2} &= \lambda_2 \\ &\vdots \\ P_{a_q} \oplus P_{b_q} &= \lambda_q \end{aligned}$$

for some surjection $\varphi : \{a_1, b_1, \ldots, a_q, b_q\} \to \{1, \ldots, r\}$

Goal

- Lower bound on the number of solutions to $\mathcal{P}$ such that $P_a \neq P_b$ for all distinct $a, b \in \{1, \ldots, r\}$

Mirror Theory

Patarin's Result

- Extremely powerful lower bound

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
Patarin	AFRICACRYPT 2008	Benes	

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
Patarin	AFRICACRYPT 2008	Benes	
Patarin	ePrint 2010/287	XoP	Concrete bound

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
Patarin	AFRICACRYPT 2008	Benes	
Patarin	ePrint 2010/287	XoP	Concrete bound
Patarin	ePrint 2010/293	Feistel	

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
Patarin	AFRICACRYPT 2008	Benes	
Patarin	ePrint 2010/287	XoP	Concrete bound
Patarin	ePrint 2010/293	Feistel	
Patarin	ePrint 2013/368	XoP	

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
Patarin	AFRICACRYPT 2008	Benes	
Patarin	ePrint 2010/287	XoP	Concrete bound
Patarin	ePrint 2010/293	Feistel	
Patarin	ePrint 2013/368	XoP	
Cogliati, Lampe, Patarin	FSE 2014	XoP^d	

Mirror Theory

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
Patarin	AFRICACRYPT 2008	Benes	
Patarin	ePrint 2010/287	XoP	Concrete bound
Patarin	ePrint 2010/293	Feistel	
Patarin	ePrint 2013/368	XoP	
Cogliati, Lampe, Patarin	FSE 2014	XoP^d	
Volte, Nachef, Marrière	ePrint 2016/136	Feistel	

Patarin's Result

- Extremely powerful lower bound
- Has remained rather unknown since introduction (2003)

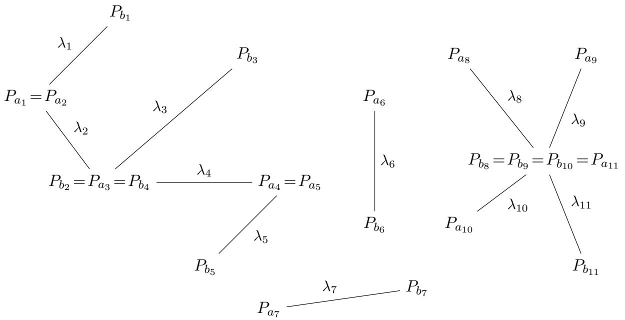
Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
Patarin	AFRICACRYPT 2008	Benes	
Patarin	ePrint 2010/287	XoP	Concrete bound
Patarin	ePrint 2010/293	Feistel	
Patarin	ePrint 2013/368	XoP	
Cogliati, Lampe, Patarin	FSE 2014	XoP^d	
Volte, Nachef, Marrière	ePrint 2016/136	Feistel	
Iwata, Mennink, Vizár	ePrint 2016/1087	CENC	

Mirror Theory

System of Equations

- r distinct unknowns $\mathcal{P} = \{P_1, \ldots, P_r\}$
- System of equations $P_{a_i} \oplus P_{b_i} = \lambda_i$
- Surjection $\varphi : \{a_1, b_1, \ldots, a_q, b_q\} \to \{1, \ldots, r\}$

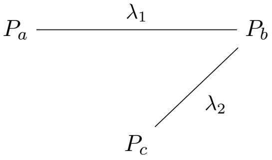
Graph Based View



Mirror Theory: Toy Example 1

- System of equations:

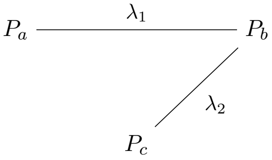
$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$



Mirror Theory: Toy Example 1

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$



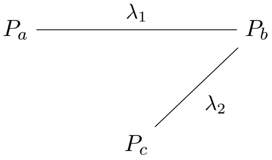
If $\lambda_1 = 0$ or $\lambda_2 = 0$ or $\lambda_1 = \lambda_2$

- Contradiction: $P_a = P_b$ or $P_b = P_c$ or $P_a = P_c$
- Scheme is degenerate

Mirror Theory: Toy Example 1

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$



If $\lambda_1 = 0$ or $\lambda_2 = 0$ or $\lambda_1 = \lambda_2$

- Contradiction: $P_a = P_b$ or $P_b = P_c$ or $P_a = P_c$
- Scheme is degenerate

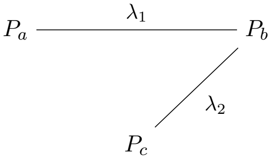
If $\lambda_1, \lambda_2 \neq 0$ and $\lambda_1 \neq \lambda_2$

- 2^n choices for P_a

Mirror Theory: Toy Example 1

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$



If $\lambda_1 = 0$ or $\lambda_2 = 0$ or $\lambda_1 = \lambda_2$

- Contradiction: $P_a = P_b$ or $P_b = P_c$ or $P_a = P_c$
- Scheme is degenerate

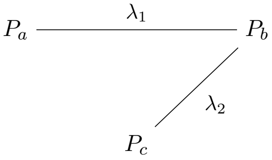
If $\lambda_1, \lambda_2 \neq 0$ and $\lambda_1 \neq \lambda_2$

- 2^n choices for P_a
- Fixes $P_b = \lambda_1 \oplus P_a$ (which is $\neq P_a$ as desired)

Mirror Theory: Toy Example 1

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$



If $\lambda_1 = 0$ or $\lambda_2 = 0$ or $\lambda_1 = \lambda_2$

- Contradiction: $P_a = P_b$ or $P_b = P_c$ or $P_a = P_c$
- Scheme is degenerate

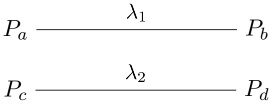
If $\lambda_1, \lambda_2 \neq 0$ and $\lambda_1 \neq \lambda_2$

- 2^n choices for P_a
- Fixes $P_b = \lambda_1 \oplus P_a$ (which is $\neq P_a$ as desired)
- Fixes $P_c = \lambda_2 \oplus P_b$ (which is $\neq P_a, P_b$ as desired)

Mirror Theory: Toy Example 2

- System of equations:

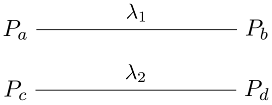
$$P_a \oplus P_b = \lambda_1$$
$$P_c \oplus P_d = \lambda_2$$



Mirror Theory: Toy Example 2

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_c \oplus P_d = \lambda_2$$



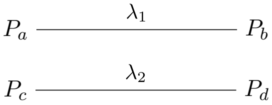
If $\lambda_1 = 0$ or $\lambda_2 = 0$

- Contradiction: $P_a = P_b$ or $P_b = P_c$
- Scheme is degenerate

Mirror Theory: Toy Example 2

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_c \oplus P_d = \lambda_2$$



If $\boldsymbol{\lambda_1 = 0}$ or $\boldsymbol{\lambda_2 = 0}$

- Contradiction: $P_a = P_b$ or $P_b = P_c$
- Scheme is degenerate

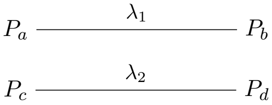
If $\boldsymbol{\lambda_1, \lambda_2 \neq 0}$

- 2^n choices for P_a (which fixes P_b)

Mirror Theory: Toy Example 2

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_c \oplus P_d = \lambda_2$$



If $\lambda_1 = 0$ or $\lambda_2 = 0$

- Contradiction: $P_a = P_b$ or $P_b = P_c$
- Scheme is degenerate

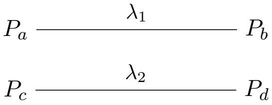
If $\lambda_1, \lambda_2 \neq 0$

- 2^n choices for P_a (which fixes P_b)
- For P_c and P_d we require
  - $P_c \neq P_a, P_b$
  - $P_d = \lambda_2 \oplus P_c \neq P_a, P_b$

Mirror Theory: Toy Example 2

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_c \oplus P_d = \lambda_2$$



If $\lambda_1 = 0$ or $\lambda_2 = 0$

- Contradiction: $P_a = P_b$ or $P_b = P_c$
- Scheme is degenerate

If $\lambda_1, \lambda_2 \neq 0$

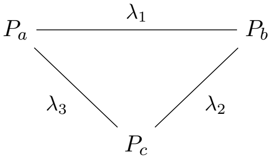
- 2^n choices for P_a (which fixes P_b)
- For P_c and P_d we require
  - $P_c \neq P_a, P_b$
  - $P_d = \lambda_2 \oplus P_c \neq P_a, P_b$
- At least $2^n - 4$ choices for P_c (which fixes P_d)

Mirror Theory: Toy Example 3

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$
$$P_c \oplus P_a = \lambda_3$$

- Assume $\lambda_i \neq 0$ and $\lambda_i \neq \lambda_j$

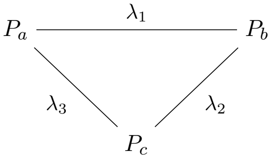


Mirror Theory: Toy Example 3

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$
$$P_c \oplus P_a = \lambda_3$$

- Assume $\lambda_i \neq 0$ and $\lambda_i \neq \lambda_j$



If $\boldsymbol{\lambda_1 \oplus \lambda_2 \oplus \lambda_3 \neq 0}$

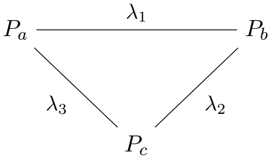
- Contradiction: equations sum to $0 = \lambda_1 \oplus \lambda_2 \oplus \lambda_3$
- Scheme contains a circle

Mirror Theory: Toy Example 3

- System of equations:

$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$
$$P_c \oplus P_a = \lambda_3$$

- Assume $\lambda_i \neq 0$ and $\lambda_i \neq \lambda_j$



If $\boldsymbol{\lambda_1 \oplus \lambda_2 \oplus \lambda_3 \neq 0}$

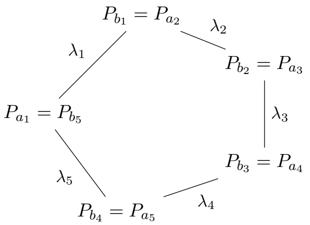
- Contradiction: equations sum to $0 = \lambda_1 \oplus \lambda_2 \oplus \lambda_3$
- Scheme contains a circle

If $\boldsymbol{\lambda_1 \oplus \lambda_2 \oplus \lambda_3 = 0}$

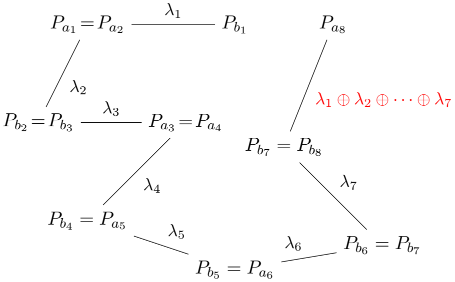
- One redundant equation, no contradiction
- Still counted as circle

Mirror Theory: Two Problematic Cases

Circle



Degeneracy



Mirror Theory: Main Result

System of Equations

- r distinct unknowns $\mathcal{P} = \{P_1, \ldots, P_r\}$
- System of equations $P_{a_i} \oplus P_{b_i} = \lambda_i$
- Surjection $\varphi : \{a_1, b_1, \ldots, a_q, b_q\} \to \{1, \ldots, r\}$

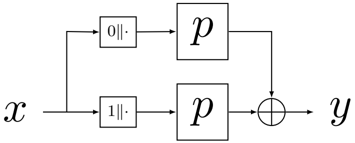
Main Result

If the system of equations is circle-free and non-degenerate, the number of solutions to $\mathcal{P}$ such that $P_a \neq P_b$ for all distinct $a, b \in \{1, \ldots, r\}$ is at least

$$\frac{(2^n)_r}{2^{nq}}$$

provided the maximum tree size ξ satisfies $(\xi - 1)^2 \cdot r \leq 2^n/67$

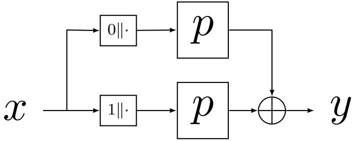
Mirror Theory Applied to XoP



General Setting

- Adversary gets transcript $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$

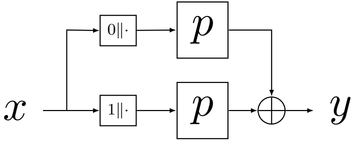
Mirror Theory Applied to XoP



General Setting

- Adversary gets transcript $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$
- Each tuple corresponds to $x_i \mapsto p(0\|x_i) =: P_{a_i}$ and
  $x_i \mapsto p(1\|x_i) =: P_{b_i}$

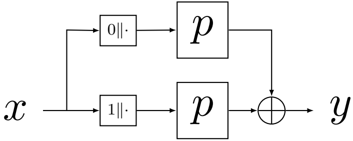
Mirror Theory Applied to XoP



General Setting

- Adversary gets transcript $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$
- Each tuple corresponds to $x_i \mapsto p(0\|x_i) =: P_{a_i}$ and
  $x_i \mapsto p(1\|x_i) =: P_{b_i}$
- System of q equations $P_{a_i} \oplus P_{b_i} = y_i$

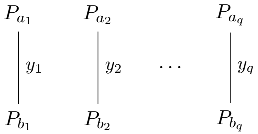
Mirror Theory Applied to XoP



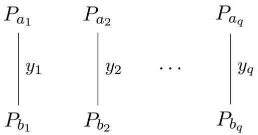
General Setting

- Adversary gets transcript $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$
- Each tuple corresponds to $x_i \mapsto p(0\|x_i) =: P_{a_i}$ and
  $x_i \mapsto p(1\|x_i) =: P_{b_i}$
- System of q equations $P_{a_i} \oplus P_{b_i} = y_i$
- Inputs to p are all distinct: $2q$ unknowns

Mirror Theory Applied to XoP



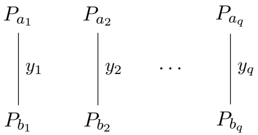
Mirror Theory Applied to XoP



Applying Mirror Theory

- Circle-free: no collisions in inputs to p
- Non-degenerate: provided that $y_i \neq 0$ for all i
  $\longrightarrow$ Call this a bad transcript
- Maximum tree size 2

Mirror Theory Applied to XoP



Applying Mirror Theory

- Circle-free: no collisions in inputs to p
- Non-degenerate: provided that $y_i \neq 0$ for all i
  $\longrightarrow$ Call this a bad transcript
- Maximum tree size 2
- If $2q \leq 2^n/67$: at least $\frac{(2^n)_{2q}}{2^{nq}}$ solutions to unknowns

Mirror Theory Applied to XoP

H-Coefficient Technique [Pat91,Pat08,CS14]

Let $\varepsilon \geq 0$ be such that for all good transcripts τ:

$$\frac{\mathbf{Pr}\left[\text{XoP gives } \tau\right]}{\mathbf{Pr}\left[f \text{ gives } \tau\right]} \geq 1 - \varepsilon$$

Then, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } f\right]$

Mirror Theory Applied to XoP

H-Coefficient Technique [Pat91,Pat08,CS14]

Let $\varepsilon \geq 0$ be such that for all good transcripts τ:

$$\frac{\mathbf{Pr}\left[\text{XoP gives } \tau\right]}{\mathbf{Pr}\left[f \text{ gives } \tau\right]} \geq 1 - \varepsilon$$

Then, $\mathbf{Adv}^{\text{prf}}_{\text{XoP}}(q) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } f\right]$

- Bad transcript: if $y_i = 0$ for some i
  - $\mathbf{Pr}\left[\text{bad transcript for } f\right] = q/2^n$

Mirror Theory Applied to XoP

H-Coefficient Technique [Pat91,Pat08,CS14]
Let $\varepsilon \geq 0$ be such that for all good transcripts τ:

$$\frac{\mathbf{Pr}\left[\text{XoP gives } \tau\right]}{\mathbf{Pr}\left[f \text{ gives } \tau\right]} \geq 1 - \varepsilon$$

Then, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } f\right]$

- Bad transcript: if $y_i = 0$ for some i
  - $\mathbf{Pr}\left[\text{bad transcript for } f\right] = q/2^n$
- For any good transcript:
  - $\mathbf{Pr}\left[\text{XoP gives } \tau\right] \geq \frac{(2^n)_{2q}}{2^{nq}} \cdot \frac{1}{(2^n)_{2q}}$

Mirror Theory Applied to XoP

H-Coefficient Technique [Pat91,Pat08,CS14]

Let $\varepsilon \geq 0$ be such that for all good transcripts τ:

$$\frac{\mathbf{Pr}\left[\text{XoP gives } \tau\right]}{\mathbf{Pr}\left[f \text{ gives } \tau\right]} \geq 1 - \varepsilon$$

Then, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } f\right]$

- Bad transcript: if $y_i = 0$ for some i
  - $\mathbf{Pr}\left[\text{bad transcript for } f\right] = q/2^n$
- For any good transcript:
  - $\mathbf{Pr}\left[\text{XoP gives } \tau\right] \geq \frac{(2^n)_{2q}}{2^{nq}} \cdot \frac{1}{(2^n)_{2q}}$
  - $\mathbf{Pr}\left[f \text{ gives } \tau\right] = \frac{1}{2^{nq}}$

Mirror Theory Applied to XoP

H-Coefficient Technique [Pat91,Pat08,CS14]

Let $\varepsilon \geq 0$ be such that for all good transcripts τ:

$$\frac{\mathbf{Pr}\left[\text{XoP gives } \tau\right]}{\mathbf{Pr}\left[f \text{ gives } \tau\right]} \geq 1 - \varepsilon$$

Then, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } f\right]$

- Bad transcript: if $y_i = 0$ for some i
  - $\mathbf{Pr}\left[\text{bad transcript for } f\right] = q/2^n$
- For any good transcript:
  - $\mathbf{Pr}\left[\text{XoP gives } \tau\right] \geq \frac{(2^n)_{2q}}{2^{nq}} \cdot \frac{1}{(2^n)_{2q}}$
  - $\mathbf{Pr}\left[f \text{ gives } \tau\right] = \frac{1}{2^{nq}}$

  $\Bigg\}\ \varepsilon = 0$

Mirror Theory Applied to XoP

H-Coefficient Technique [Pat91,Pat08,CS14]

Let $\varepsilon \geq 0$ be such that for all good transcripts τ:

$$\frac{\mathbf{Pr}\left[\text{XoP gives } \tau\right]}{\mathbf{Pr}\left[f \text{ gives } \tau\right]} \geq 1 - \varepsilon$$

Then, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q) \leq \varepsilon + \mathbf{Pr}\left[\text{bad transcript for } f\right]$

- Bad transcript: if $y_i = 0$ for some i
  - $\mathbf{Pr}\left[\text{bad transcript for } f\right] = q/2^n$
- For any good transcript:
  - $\mathbf{Pr}\left[\text{XoP gives } \tau\right] \geq \frac{(2^n)_{2q}}{2^{nq}} \cdot \frac{1}{(2^n)_{2q}}$
  - $\mathbf{Pr}\left[f \text{ gives } \tau\right] = \frac{1}{2^{nq}}$

  $\Big\}\ \varepsilon = 0$

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP}}(q) \leq q/2^n$$

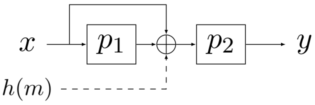
New Look at Mirror Theory

Encrypted Davies-Meyer and Its Dual:
Towards Optimal Security Using Mirror Theory

Mennink, Neves, CRYPTO 2017

- Refurbish and modernize mirror theory
- Prove optimal PRF security of:

E(WC)DM [CS16]



EDMD