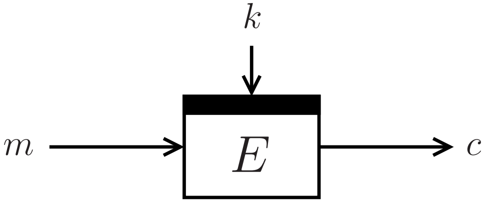
Tweakable Blockciphers and Beyond Birthday Bound Security

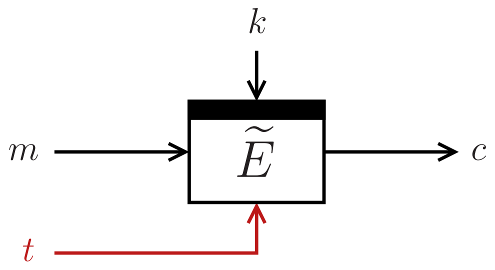
Bart Mennink
Radboud University (The Netherlands)

8th Asian Workshop on Symmetric Key Cryptography
November 15, 2018

Tweakable Blockciphers

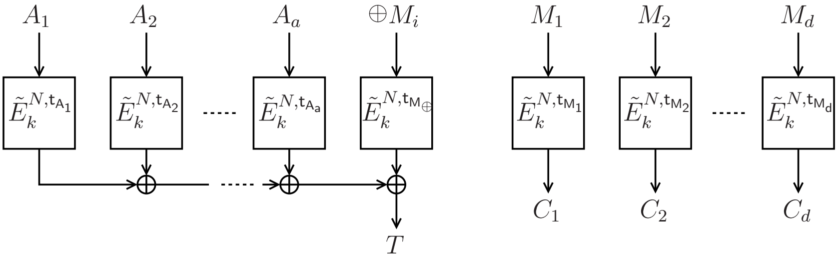


Tweakable Blockciphers



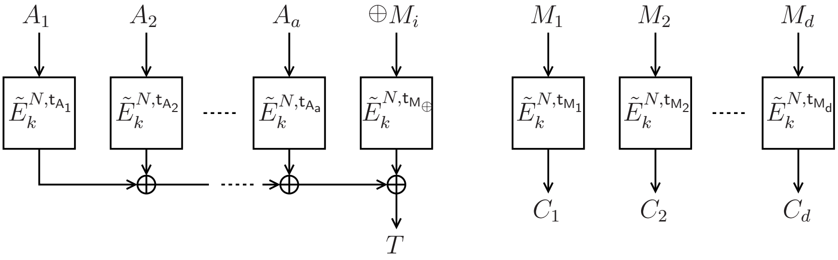
- Tweak: flexibility to the cipher
- Each tweak gives different permutation

Tweakable Blockciphers in OCBx



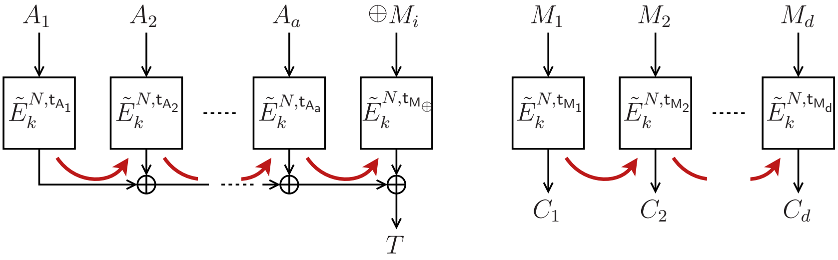
- Generalized OCB by Rogaway et al. [RBBK01,Rog04,KR11]

Tweakable Blockciphers in OCBx



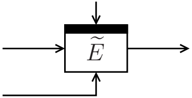
- Generalized OCB by Rogaway et al. [RBBK01,Rog04,KR11]
- Internally based on tweakable blockcipher $\widetilde{E}$
  - Tweak (N, index) is unique for every evaluation
  - Different blocks always transformed under different tweak

Tweakable Blockciphers in OCBx

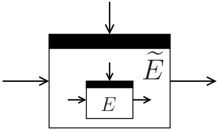


- Generalized OCB by Rogaway et al. [RBBK01,Rog04,KR11]
- Internally based on tweakable blockcipher $\widetilde{E}$
  - Tweak (N, index) is unique for every evaluation
  - Different blocks always transformed under different tweak
- Change of tweak should be efficient

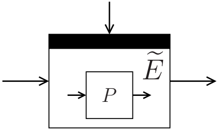
Tweakable Blockcipher Designs



Dedicated

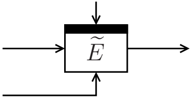


Blockcipher-Based



Permutation-Based

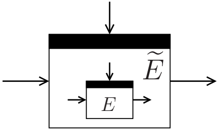
Tweakable Blockcipher Designs in CAESAR



Dedicated

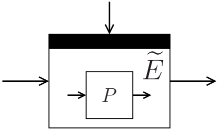
KIASU,
Joltik, **SCREAM**,

Deoxys



Blockcipher-Based

CBA, COBRA, iFeed, Marble
OMD, **POET**, **SHELL**,
AEZ, **OTR**,
COPA/ELmD, ***OCB***



Permutation-Based

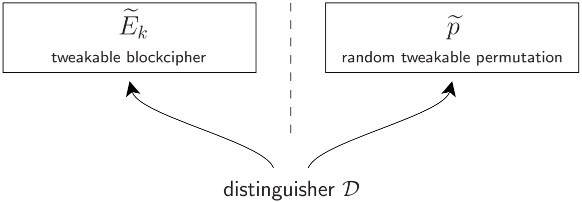
Prøst,
Minalpher

first round, **second round**, **third round**, ***final round***

Dedicated Tweakable Blockciphers

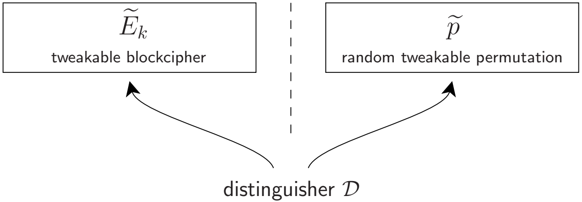
- Hasty Pudding Cipher [Sch98]
  - AES submission, "first tweakable cipher"
- Mercy [Cro01]
  - Disk encryption
- Threefish [FLS+07]
  - SHA-3 submission Skein
- TWEAKEY framework [JNP14]
  - Four CAESAR submissions
  - SKINNY & MANTIS

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

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

Outline

Tweakable Blockciphers Based on Masking

- Intuition
- State of the Art
- Improved Efficiency

Beyond Birthday Bound Tweakable Blockciphers

- State of the Art
- Tight Security of Cascaded LRW_2?
- Improved Attack
- Improved Security Bound

Conclusion

Outline

Tweakable Blockciphers Based on Masking

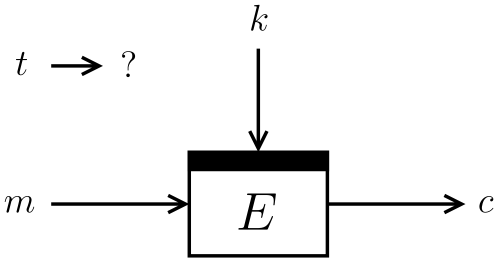
- Intuition
- State of the Art
- Improved Efficiency

Beyond Birthday Bound Tweakable Blockciphers

- State of the Art
- Tight Security of Cascaded LRW_2?
- Improved Attack
- Improved Security Bound

Conclusion

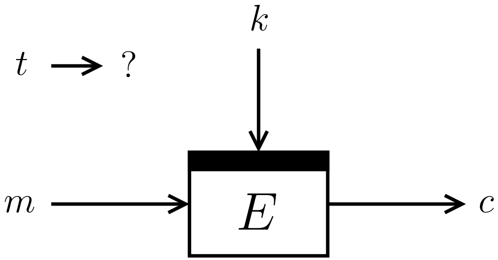
Intuition: Design



- Consider a blockcipher E with κ-bit key and n-bit state

How to mingle the tweak into the evaluation?

Intuition: Design



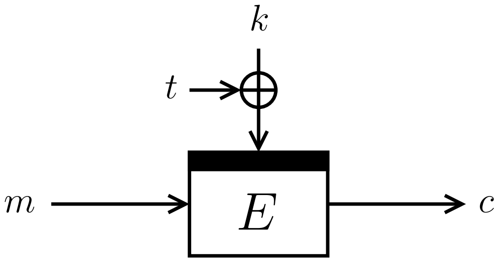
- Consider a blockcipher E with κ-bit key and n-bit state

How to mingle the tweak into the evaluation?

blend it with the key

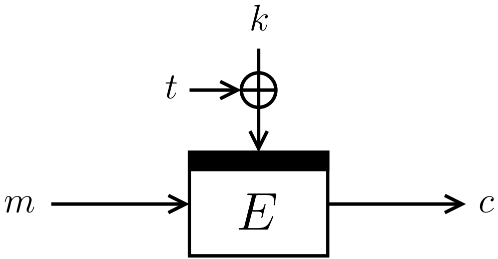
blend it with the state

Intuition: Design



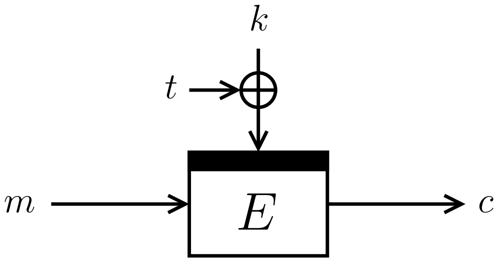
- Blending tweak and key works...
- ... but: careful with related-key attacks!

Intuition: Design



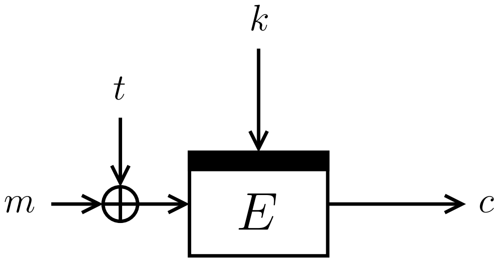
- Blending tweak and key works...
- ... but: careful with related-key attacks!
- For $\oplus$-mixing, key can be recovered in $2^{\kappa/2}$ evaluations
- Scheme is insecure if E is Even-Mansour

Intuition: Design



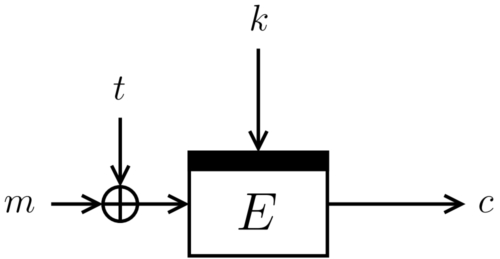
- Blending tweak and key works...
- ... but: careful with related-key attacks!
- For $\oplus$-mixing, key can be recovered in $2^{\kappa/2}$ evaluations
- Scheme is insecure if E is Even-Mansour
- TWEAKEY blending [JNP14] is more advanced

Intuition: Design



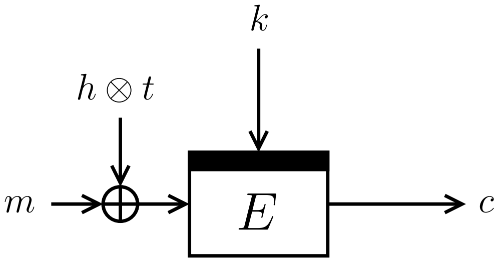
- Simple blending of tweak and state does not work

Intuition: Design



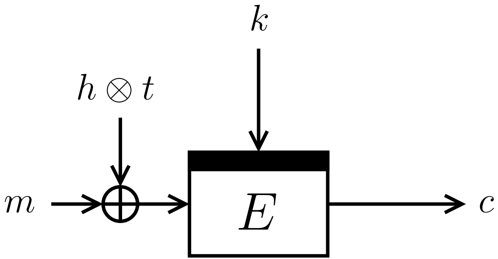
- Simple blending of tweak and state does not work
  - $\widetilde{E}_k(t, m) = \widetilde{E}_k(t \oplus C, m \oplus C)$

Intuition: Design



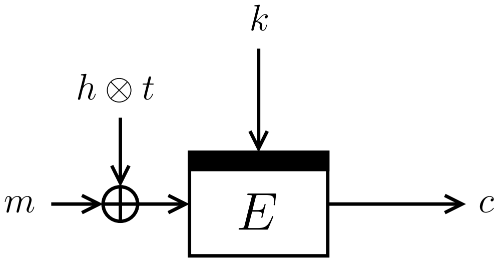
- Simple blending of tweak and state does not work
  - $\widetilde{E}_k(t, m) = \widetilde{E}_k(t \oplus C, m \oplus C)$
- Some secrecy required: h

Intuition: Design



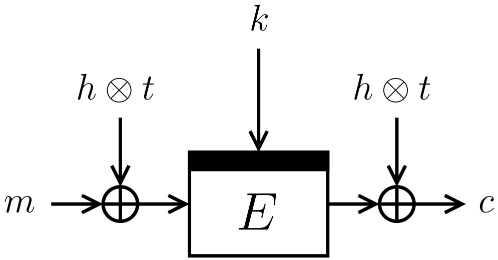
- Simple blending of tweak and state does not work
  - $\widetilde{E}_k(t, m) = \widetilde{E}_k(t \oplus C, m \oplus C)$
- Some secrecy required: h
- Still does not work if adversary has access to $\widetilde{E}_k^{-1}$

Intuition: Design



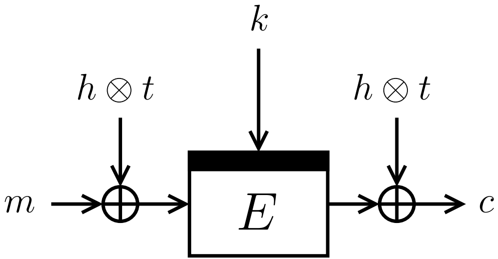
- Simple blending of tweak and state does not work
  - $\widetilde{E}_k(t, m) = \widetilde{E}_k(t \oplus C, m \oplus C)$
- Some secrecy required: h
- Still does not work if adversary has access to $\widetilde{E}_k^{-1}$
  - $\widetilde{E}_k^{-1}(t, c) \oplus \widetilde{E}_k^{-1}(t \oplus C, c) = h \otimes C$

Intuition: Design



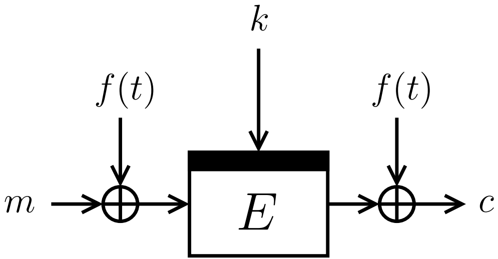
- Simple blending of tweak and state does not work
  - $\widetilde{E}_k(t, m) = \widetilde{E}_k(t \oplus C, m \oplus C)$
- Some secrecy required: h
- Still does not work if adversary has access to $\widetilde{E}_k^{-1}$
  - $\widetilde{E}_k^{-1}(t, c) \oplus \widetilde{E}_k^{-1}(t \oplus C, c) = h \otimes C$
  - Two-sided masking necessary

Intuition: Design



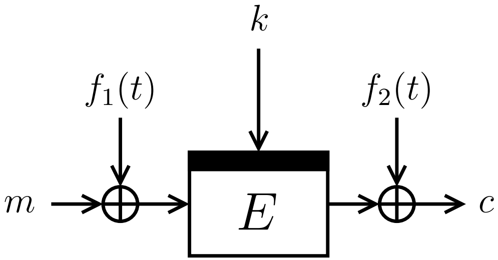
- Two-sided secret masking seems to work
- Can we generalize?

Intuition: Design



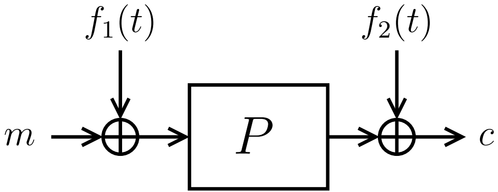
- Two-sided secret masking seems to work
- Can we generalize?
- Generalizing masking? Depends on function f

Intuition: Design



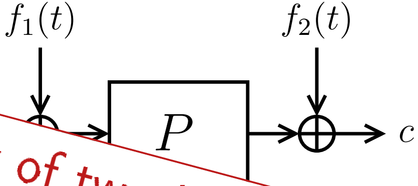
- Two-sided secret masking seems to work
- Can we generalize?
- Generalizing masking? Depends on function f
- Variation in masking? Depends on functions f_1, f_2

Intuition: Design



- Two-sided secret masking seems to work
- Can we generalize?
- Generalizing masking? Depends on function f
- Variation in masking? Depends on functions f_1, f_2
- Releasing secrecy in E? Usually no problem

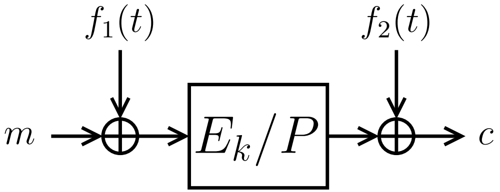
Intuition: Design



Majority of tweakable blockciphers follow mask-E_k/P-mask principle

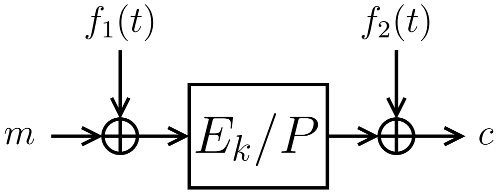
- Two-sided secret ma...
- Can we generalize?
- Generalizing masking? Depends on function f
- Variation in masking? Depends on functions f_1, f_2
- Releasing secrecy in E? Usually no problem

Intuition: Analysis



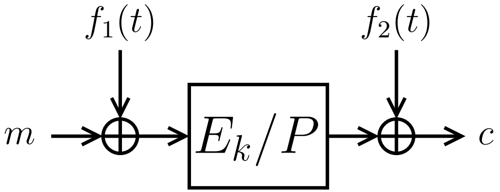
- $\widetilde{E}_k$ should "look like" random permutation for every t
- Consider adversary $\mathcal{D}$ that makes q evaluations of $\widetilde{E}_k$

Intuition: Analysis



- $\widetilde{E}_k$ should "look like" random permutation for every t
- Consider adversary $\mathcal{D}$ that makes q evaluations of $\widetilde{E}_k$
- Step 1:
  - How many evaluations does $\mathcal{D}$ need at most?
  - Boils down to finding generic attacks

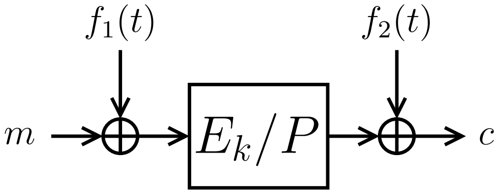
Intuition: Analysis



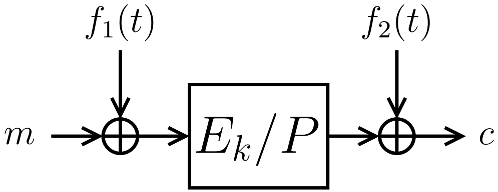
- $\widetilde{E}_k$ should "look like" random permutation for every t
- Consider adversary $\mathcal{D}$ that makes q evaluations of $\widetilde{E}_k$

- Step 1:
  - How many evaluations does $\mathcal{D}$ need at most?
  - Boils down to finding generic attacks
- Step 2:
  - How many evaluations does $\mathcal{D}$ need at least?
  - Boils down to provable security

Intuition: Analysis



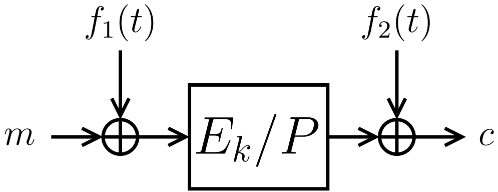
Intuition: Analysis



- For any two queries (t, m, c), (t', m', c'):

$$m \oplus f_1(t) = m' \oplus f_1(t') \implies c \oplus f_2(t) = c' \oplus f_2(t')$$

Intuition: Analysis

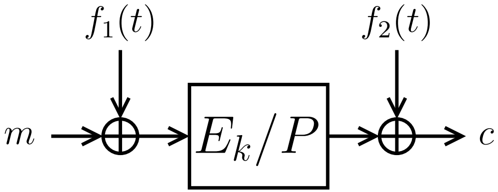


- For any two queries (t, m, c), (t', m', c'):

$$m \oplus f_1(t) = m' \oplus f_1(t') \Longrightarrow c \oplus f_2(t) = c' \oplus f_2(t')$$

- Unlikely to happen for random family of permutations

Intuition: Analysis

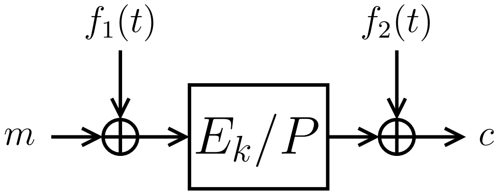


- For any two queries (t, m, c), (t', m', c'):

$$m \oplus f_1(t) = m' \oplus f_1(t') \implies c \oplus f_2(t) = c' \oplus f_2(t')$$

- Unlikely to happen for random family of permutations
- Implication still holds with difference C xored to m, m'

Intuition: Analysis



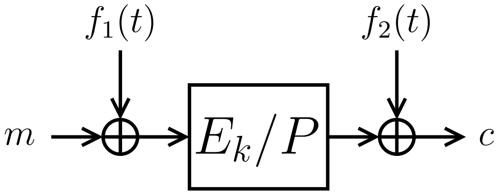
- For any two queries (t, m, c), (t', m', c'):

$$m \oplus f_1(t) = m' \oplus f_1(t') \implies c \oplus f_2(t) = c' \oplus f_2(t')$$

- Unlikely to happen for random family of permutations
- Implication still holds with difference C xored to m, m'

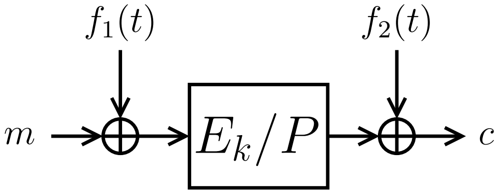
Scheme can be broken in $\approx 2^{n/2}$ evaluations

Intuition: Analysis



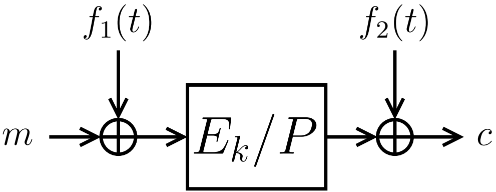
- The fun starts here!
- More technical and often more involved

Intuition: Analysis



- The fun starts here!
- More technical and often more involved
- Typical approach:
  - Consider any transcript τ an adversary may see
  - Most τ's should be equally likely in both worlds
  - Odd ones should happen with very small probability

Intuition: Analysis



- The fun starts here!
- More technical and often more involved
- Typical approach:
  - Consider any transcript τ an adversary may see
  - Most τ's should be equally likely in both worlds
  - Odd ones should happen with very small probability

All constructions of this kind: secure up to $\approx 2^{n/2}$ evaluations

Outline

Tweakable Blockciphers Based on Masking

- Intuition
- State of the Art
- Improved Efficiency

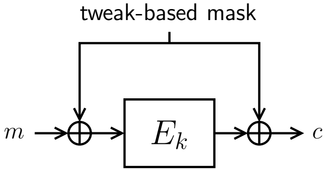
Beyond Birthday Bound Tweakable Blockciphers

- State of the Art
- Tight Security of Cascaded LRW_2?
- Improved Attack
- Improved Security Bound

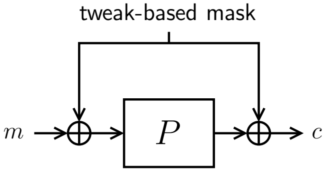
Conclusion

Tweakable Blockciphers Based on Masking

Blockcipher-Based

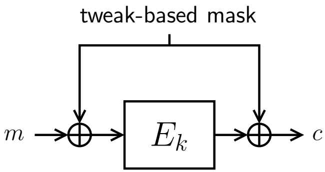


Permutation-Based



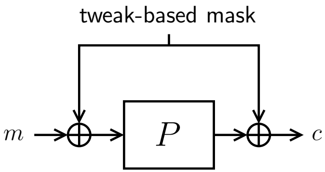
Tweakable Blockciphers Based on Masking

Blockcipher-Based



typically 128 bits

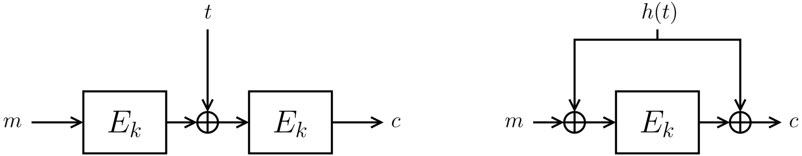
Permutation-Based



much larger: 256-1600 bits

Original Constructions

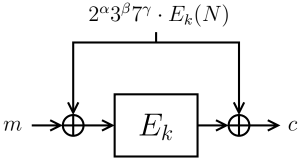
- LRW_1 and LRW_2 by Liskov et al. [LRW02]:



- h is XOR-universal hash
  - E.g., $h(t) = h \otimes t$ for n-bit "key" h

Powering-Up Masking (XEX)

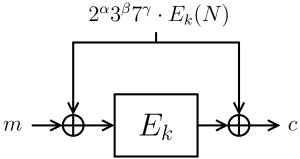
- XEX by Rogaway [Rog04]:



- $(\alpha, \beta, \gamma, N)$ is tweak (simplified)

Powering-Up Masking (XEX)

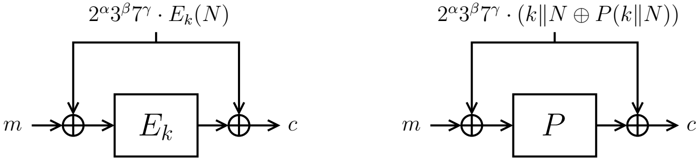
- XEX by Rogaway [Rog04]:



- $(\alpha, \beta, \gamma, N)$ is tweak (simplified)
- Used in OCB2 and ± 14 CAESAR candidates

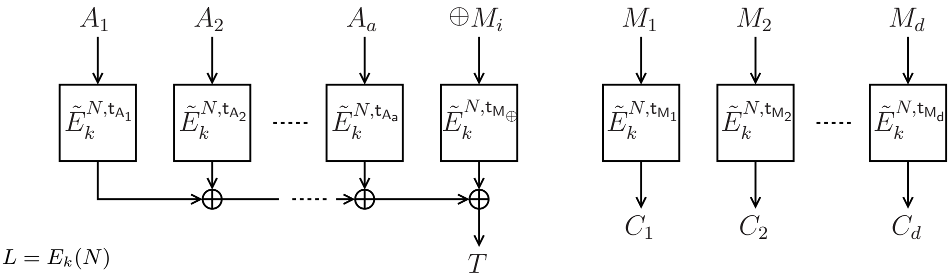
Powering-Up Masking (XEX)

- XEX by Rogaway [Rog04]:

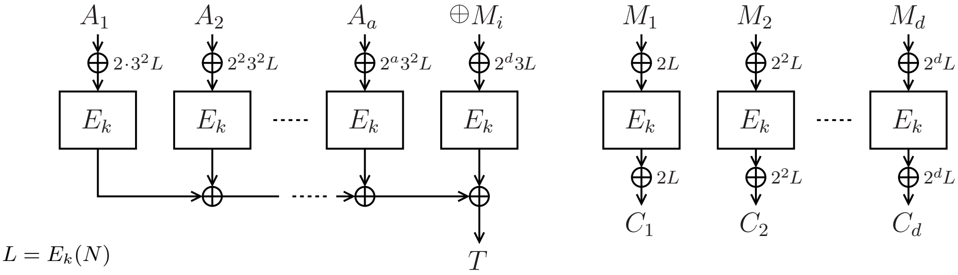


- $(\alpha, \beta, \gamma, N)$ is tweak (simplified)
- Used in OCB2 and ± 14 CAESAR candidates
- Permutation-based variants in Minalpher and Prøst (generalized by Cogliati et al. [CLS15])

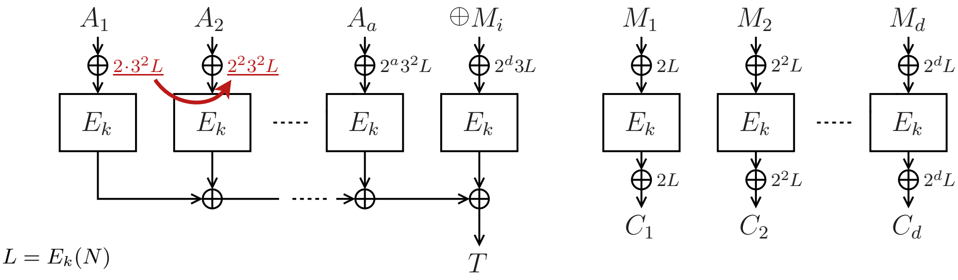
Powering-Up Masking in OCB2-Like Construction



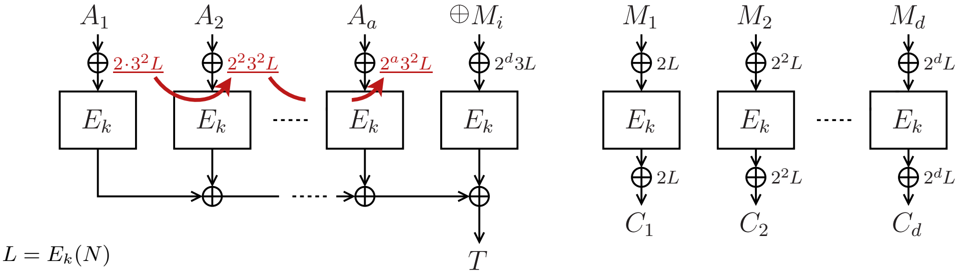
Powering-Up Masking in OCB2-Like Construction



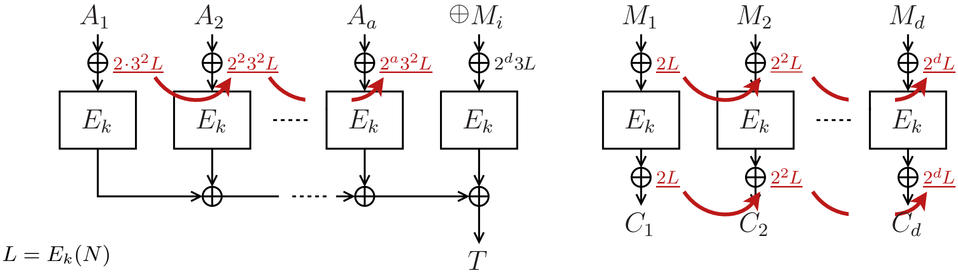
Powering-Up Masking in OCB2-Like Construction



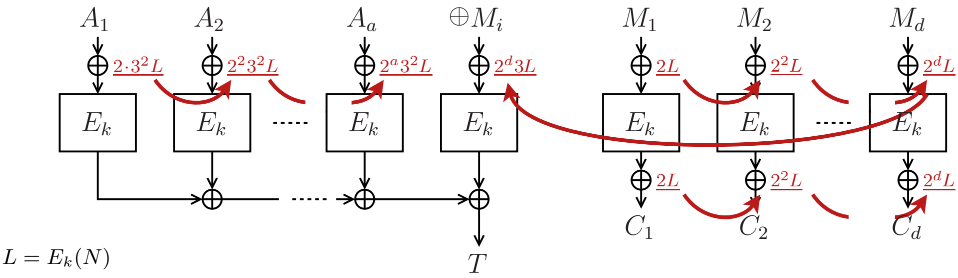
Powering-Up Masking in OCB2-Like Construction



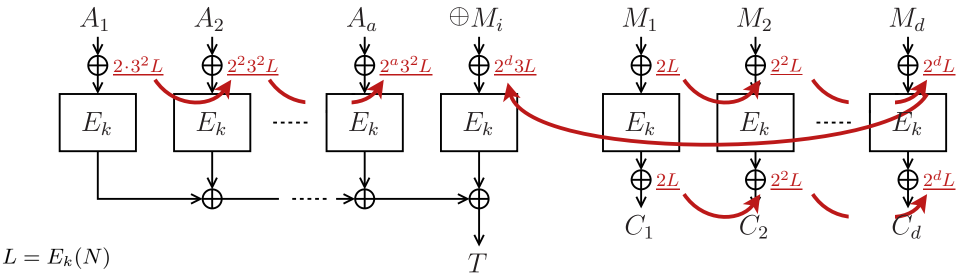
Powering-Up Masking in OCB2-Like Construction



Powering-Up Masking in OCB2-Like Construction



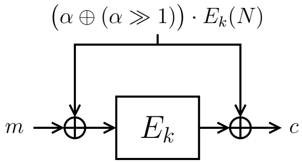
Powering-Up Masking in OCB2-Like Construction



- Update of mask:
    - Shift and conditional XOR
- Variable time computation
- Expensive on certain platforms

Gray Code Masking

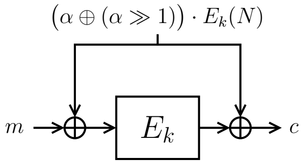
- OCB1 and OCB3 use Gray Codes:



- (α, N) is tweak
- Updating: $G(\alpha) = G(\alpha - 1) \oplus 2^{\mathsf{ntz}(\alpha)}$

Gray Code Masking

- OCB1 and OCB3 use Gray Codes:



- (α, N) is tweak
- Updating: $G(\alpha) = G(\alpha - 1) \oplus 2^{\mathsf{ntz}(\alpha)}$
  - Single XOR
  - Logarithmic amount of field doublings (precomputed)
- More efficient than powering-up [KR11]

Outline

Tweakable Blockciphers Based on Masking

- Intuition
- State of the Art
- Improved Efficiency

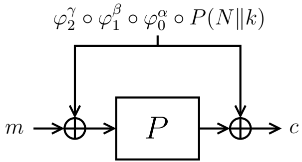
Beyond Birthday Bound Tweakable Blockciphers

- State of the Art
- Tight Security of Cascaded LRW_2?
- Improved Attack
- Improved Security Bound

Conclusion

Masked Even-Mansour (MEM)

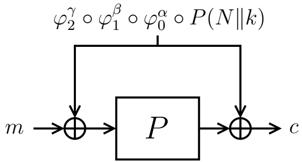
- MEM by Granger et al. [GJMN16]:



- φ_i are fixed LFSRs, $(\alpha, \beta, \gamma, N)$ is tweak (simplified)

Masked Even-Mansour (MEM)

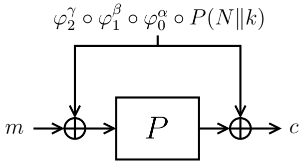
- MEM by Granger et al. [GJMN16]:



- φ_i are fixed LFSRs, $(\alpha, \beta, \gamma, N)$ is tweak (simplified)
- Combines advantages of:
  - Powering-up masking
  - Word-based LFSRs

Masked Even-Mansour (MEM)

- MEM by Granger et al. [GJMN16]:



- φ_i are fixed LFSRs, $(\alpha, \beta, \gamma, N)$ is tweak (simplified)
- Combines advantages of:
  - Powering-up masking
  - Word-based LFSRs
- Simpler, constant-time (by default), more efficient

MEM: Design Considerations

- Particularly suited for large states (permutations)
- Low operation counts by clever choice of LFSR

MEM: Design Considerations

- Particularly suited for large states (permutations)
- Low operation counts by clever choice of LFSR
- Sample LFSRs (state size b as n words of w bits):

b	w	n	φ
128	8	16	$(x_1, \ldots, x_{15}, (x_0 \lll 1) \oplus (x_9 \gg 1) \oplus (x_{10} \ll 1))$
128	32	4	$(x_1, \ldots, x_3, (x_0 \lll 5) \oplus x_1 \oplus (x_1 \ll 13))$
128	64	2	$(x_1, (x_0 \lll 11) \oplus x_1 \oplus (x_1 \ll 13))$
256	64	4	$(x_1, \ldots, x_3, (x_0 \lll 3) \oplus (x_3 \gg 5))$
512	32	16	$(x_1, \ldots, x_{15}, (x_0 \lll 5) \oplus (x_3 \gg 7))$
512	64	8	$(x_1, \ldots, x_7, (x_0 \lll 29) \oplus (x_1 \ll 9))$
1024	64	16	$(x_1, \ldots, x_{15}, (x_0 \lll 53) \oplus (x_5 \ll 13))$
1600	32	50	$(x_1, \ldots, x_{49}, (x_0 \lll 3) \oplus (x_{23} \gg 3))$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

MEM: Design Considerations

- Particularly suited for large states (permutations)
- Low operation counts by clever choice of LFSR
- Sample LFSRs (state size b as n words of w bits):

b	w	n	φ
128	8	16	$(x_1, \ldots, x_{15}, (x_0 \lll 1) \oplus (x_9 \gg 1) \oplus (x_{10} \ll 1))$
128	32	4	$(x_1, \ldots, x_3, (x_0 \lll 5) \oplus x_1 \oplus (x_1 \ll 13))$
128	64	2	$(x_1, (x_0 \lll 11) \oplus x_1 \oplus (x_1 \ll 13))$
256	64	4	$(x_1, \ldots, x_3, (x_0 \lll 3) \oplus (x_3 \gg 5))$
512	32	16	$(x_1, \ldots, x_{15}, (x_0 \lll 5) \oplus (x_3 \gg 7))$
512	64	8	$(x_1, \ldots, x_7, (x_0 \lll 29) \oplus (x_1 \ll 9))$
1024	64	16	$(x_1, \ldots, x_{15}, (x_0 \lll 53) \oplus (x_5 \ll 13))$
1600	32	50	$(x_1, \ldots, x_{49}, (x_0 \lll 3) \oplus (x_{23} \gg 3))$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

- Work exceptionally well for ARX primitives

MEM: Uniqueness of Masking

- Intuitively, masking goes well as long as

$$\varphi_2^{\gamma} \circ \varphi_1^{\beta} \circ \varphi_0^{\alpha} \neq \varphi_2^{\gamma'} \circ \varphi_1^{\beta'} \circ \varphi_0^{\alpha'}$$

  for any $(\alpha, \beta, \gamma) \neq (\alpha', \beta', \gamma')$
- Challenge: set proper domain for (α, β, γ)
- Requires computation of discrete logarithms

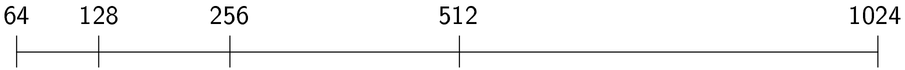
MEM: Uniqueness of Masking

- Intuitively, masking goes well as long as

$$\varphi_2^{\gamma} \circ \varphi_1^{\beta} \circ \varphi_0^{\alpha} \neq \varphi_2^{\gamma'} \circ \varphi_1^{\beta'} \circ \varphi_0^{\alpha'}$$

  for any $(\alpha, \beta, \gamma) \neq (\alpha', \beta', \gamma')$

- Challenge: set proper domain for (α, β, γ)
- Requires computation of discrete logarithms

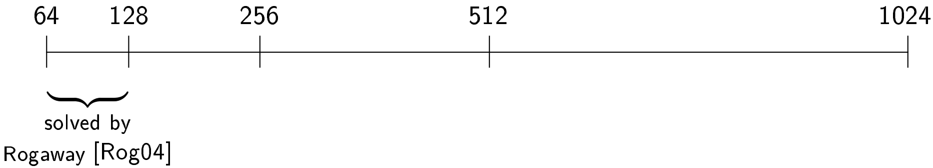


MEM: Uniqueness of Masking

- Intuitively, masking goes well as long as

$$\varphi_2^{\gamma} \circ \varphi_1^{\beta} \circ \varphi_0^{\alpha} \neq \varphi_2^{\gamma'} \circ \varphi_1^{\beta'} \circ \varphi_0^{\alpha'}$$

  for any $(\alpha, \beta, \gamma) \neq (\alpha', \beta', \gamma')$
- Challenge: set proper domain for (α, β, γ)
- Requires computation of discrete logarithms

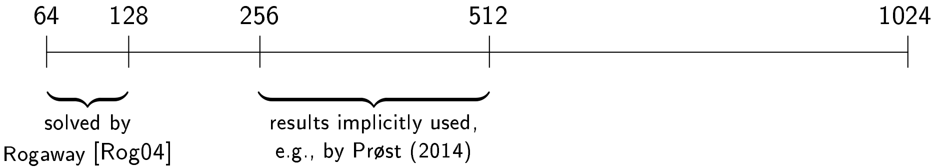


MEM: Uniqueness of Masking

- Intuitively, masking goes well as long as

$$\varphi_2^{\gamma} \circ \varphi_1^{\beta} \circ \varphi_0^{\alpha} \neq \varphi_2^{\gamma'} \circ \varphi_1^{\beta'} \circ \varphi_0^{\alpha'}$$

  for any $(\alpha, \beta, \gamma) \neq (\alpha', \beta', \gamma')$
- Challenge: set proper domain for (α, β, γ)
- Requires computation of discrete logarithms

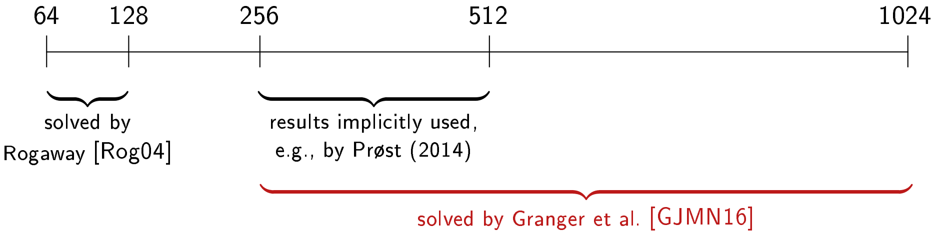


MEM: Uniqueness of Masking

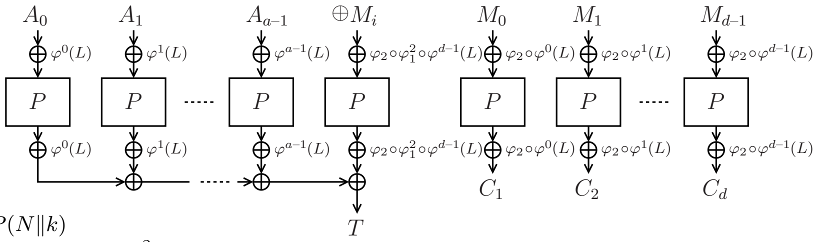
- Intuitively, masking goes well as long as

$$\varphi_2^{\gamma} \circ \varphi_1^{\beta} \circ \varphi_0^{\alpha} \neq \varphi_2^{\gamma'} \circ \varphi_1^{\beta'} \circ \varphi_0^{\alpha'}$$

  for any $(\alpha, \beta, \gamma) \neq (\alpha', \beta', \gamma')$
- Challenge: set proper domain for (α, β, γ)
- Requires computation of discrete logarithms



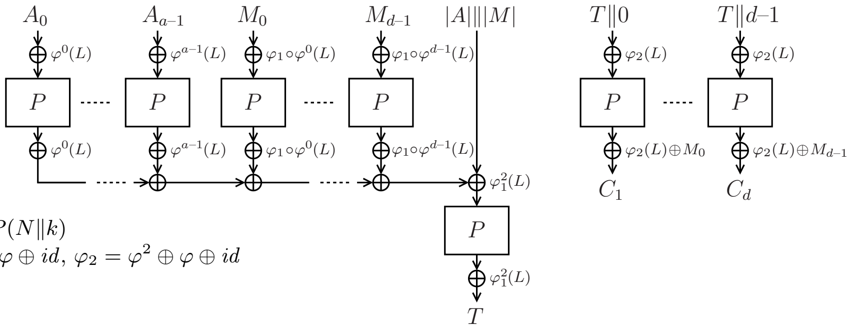
Application to AE: OPP



$L = P(N \| k)$
$\varphi_1 = \varphi \oplus id$, $\varphi_2 = \varphi^2 \oplus \varphi \oplus id$

- Offset Public Permutation (OPP)
- Generalization of OCB3:
  - Permutation-based
  - More efficient MEM masking
- Security against nonce-respecting adversaries
- 0.55 cpb with reduced-round BLAKE2b

Application to AE: MRO



$L = P(N\|k)$
$\varphi_1 = \varphi \oplus id$, $\varphi_2 = \varphi^2 \oplus \varphi \oplus id$

- Misuse-Resistant OPP (MRO)
- Fully nonce-misuse resistant version of OPP
- 1.06 cpb with reduced-round BLAKE2b

Outline

Tweakable Blockciphers Based on Masking

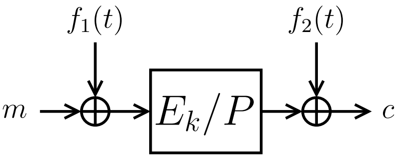
- Intuition
- State of the Art
- Improved Efficiency

Beyond Birthday Bound Tweakable Blockciphers

- State of the Art
- Tight Security of Cascaded LRW_2?
- Improved Attack
- Improved Security Bound

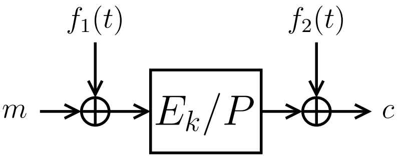
Conclusion

Beyond Birthday Bound Tweakable Blockciphers



- "Birthday bound" $2^{n/2}$ security at best
- Overlying modes inherit security bound

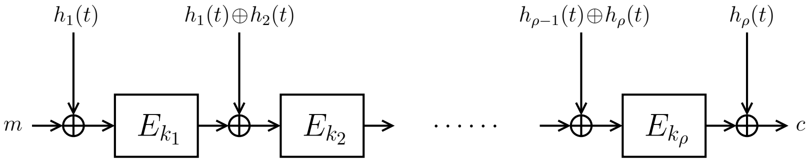
Beyond Birthday Bound Tweakable Blockciphers



- "Birthday bound" $2^{n/2}$ security at best
- Overlying modes inherit security bound

- If n is large enough $\longrightarrow$ no problem
- If n is small $\longrightarrow$ "beyond birthday bound" solutions
  - Tweak-rekeying [Min09,Men15,WGZ+16,JLM+17,Cog18,LL18]
  - Cascading (now)

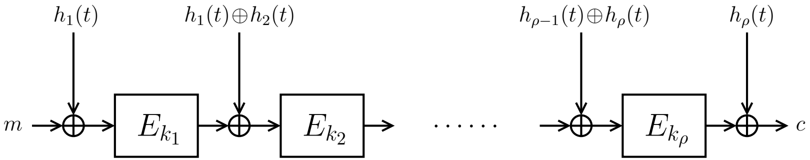
Cascading LRW_2's



- $\mathsf{LRW}_2[\rho]$: 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

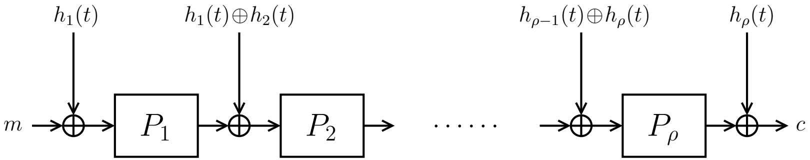


- $\mathsf{LRW}_2[\rho]$: concatenation of ρ LRW_2's
- $k_1, \ldots, k_\rho$ and $h_1, \ldots, h_\rho$ independent

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

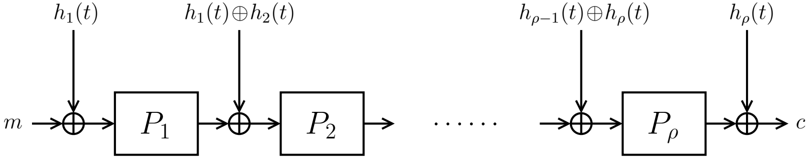
- $\rho = 2$: secure up to $2^{2n/3}$ queries [LST12,Pro14]
- $\rho \geq 2$ even: secure up to $2^{\rho n/(\rho+2)}$ queries [LS13]
- Best attack: 2^n queries

Cascading TEM's



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

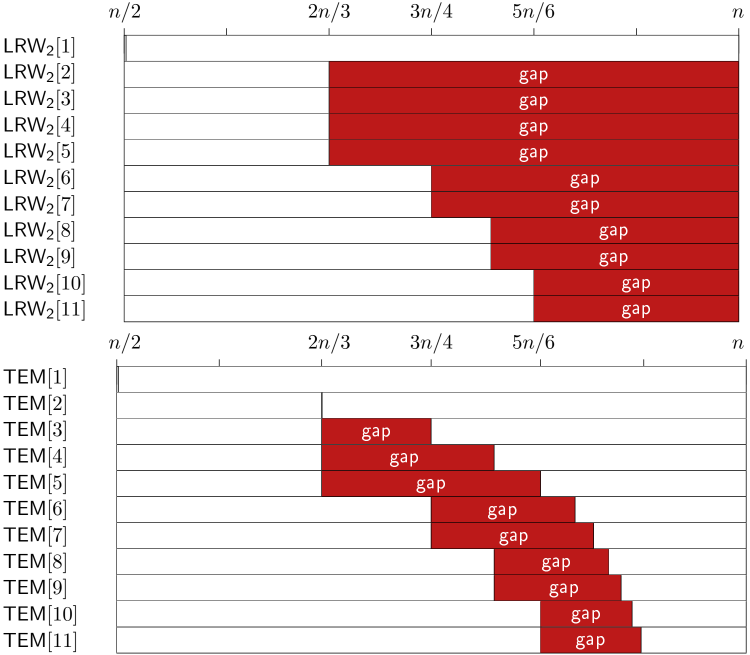
Cascading TEM's



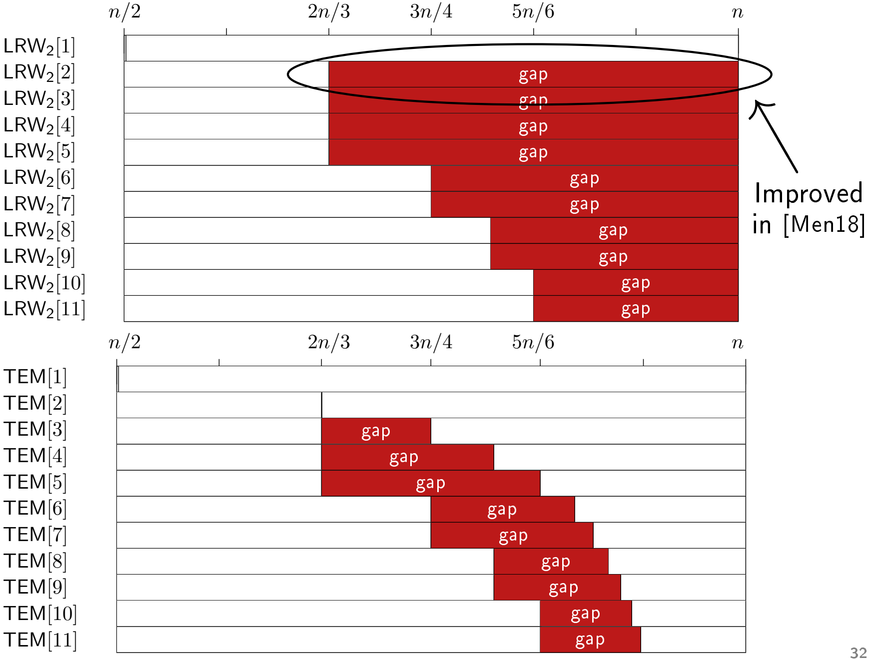
- TEM$[\rho]$: concatenation of ρ TEM's
- $P_1, \ldots, P_\rho$ and $h_1, \ldots, h_\rho$ independent

- $\rho = 2$: 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



Outline

Tweakable Blockciphers Based on Masking

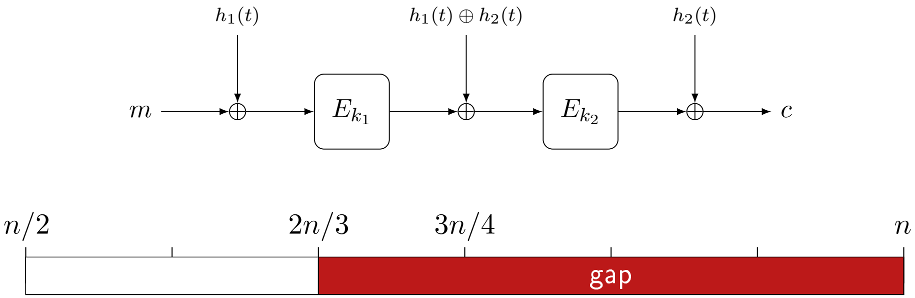
- Intuition
- State of the Art
- Improved Efficiency

Beyond Birthday Bound Tweakable Blockciphers

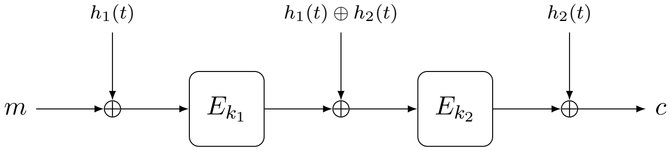
- State of the Art
- Tight Security of Cascaded LRW_2?
- Improved Attack
- Improved Security Bound

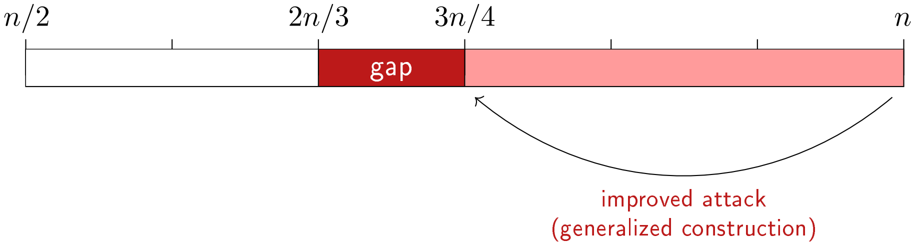
Conclusion

Tight Security of Cascaded LRW_2?

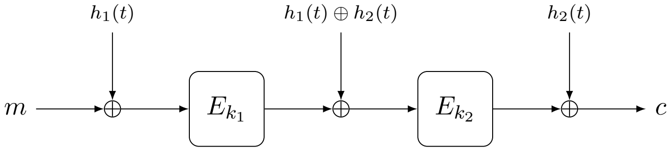


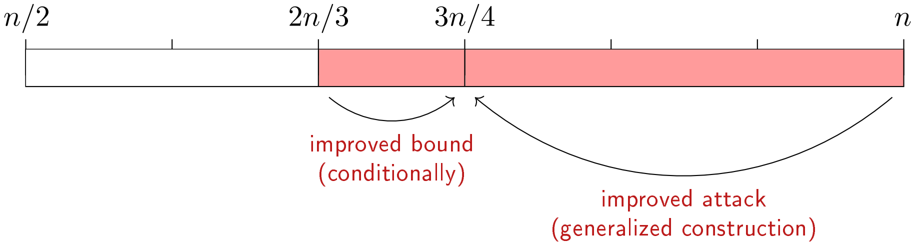
Tight Security of Cascaded LRW_2?



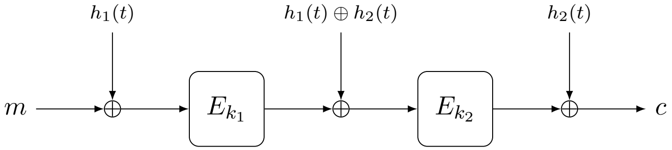


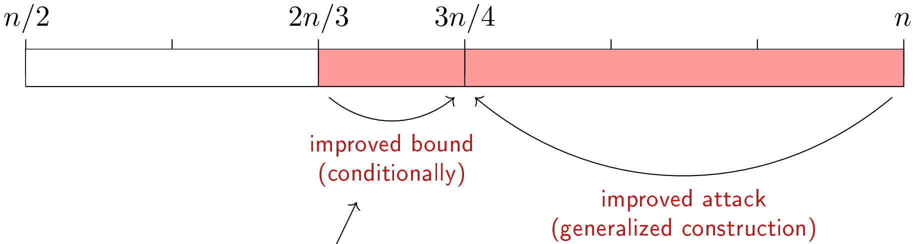
Tight Security of Cascaded LRW_2?





Tight Security of Cascaded LRW_2?





carries over to $\mathsf{LRW}_2[3]$–$\mathsf{LRW}_2[5]$

Outline

Tweakable Blockciphers Based on Masking

- Intuition
- State of the Art
- Improved Efficiency

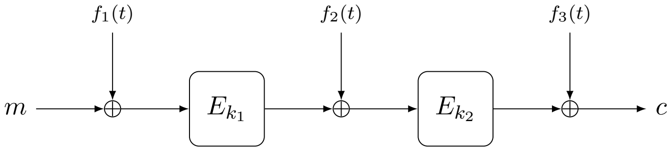
Beyond Birthday Bound Tweakable Blockciphers

- State of the Art
- Tight Security of Cascaded LRW_2?
- Improved Attack
- Improved Security Bound

Conclusion

Improved Attack

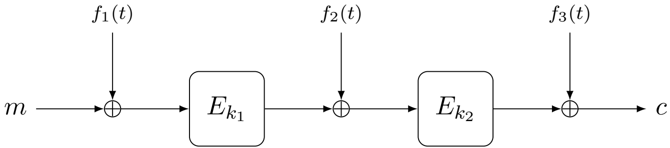
- GCL (Generalized Cascaded LRW$_2$):



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

Improved Attack

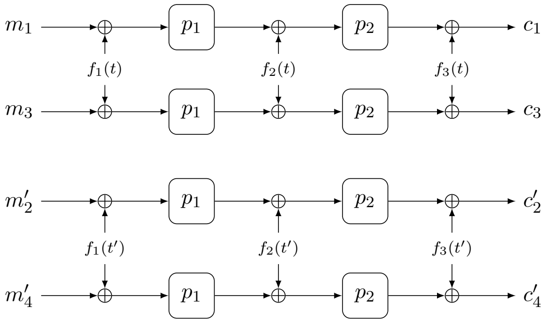
- GCL (Generalized Cascaded LRW$_2$):



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

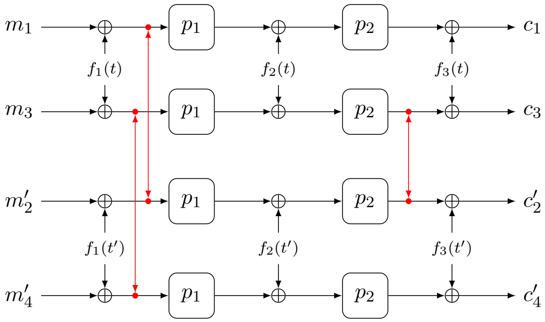
Generic distinguishing attack in $2n^{1/2}2^{3n/4}$ evaluations

Improved Attack: Rationale



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

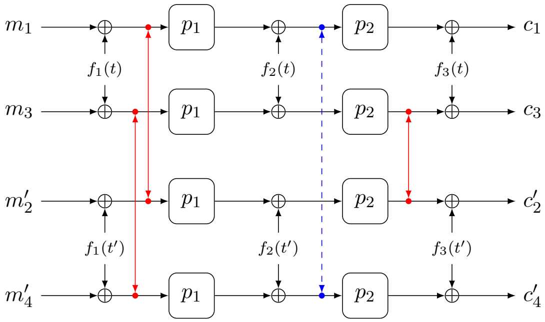
Improved Attack: Rationale



- 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



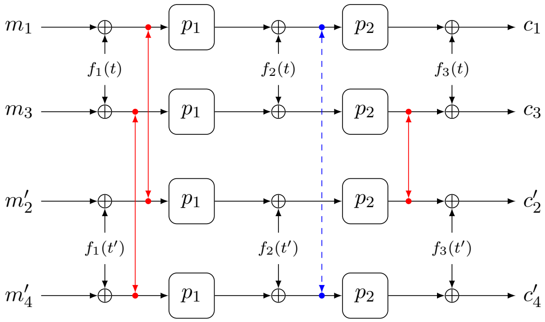
- Distinguisher $\mathcal{D}$ makes various queries for two different tweaks: t and t'
- Suppose it makes 4 queries such that

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

- 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

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

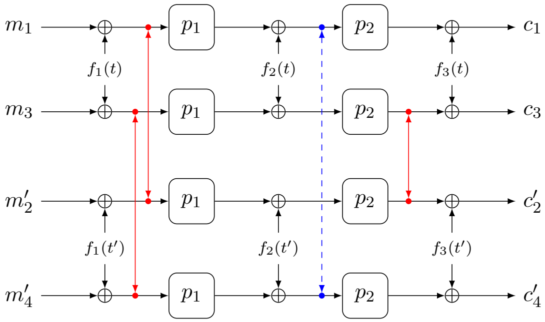
- Necessarily,

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

- Stated differently:

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

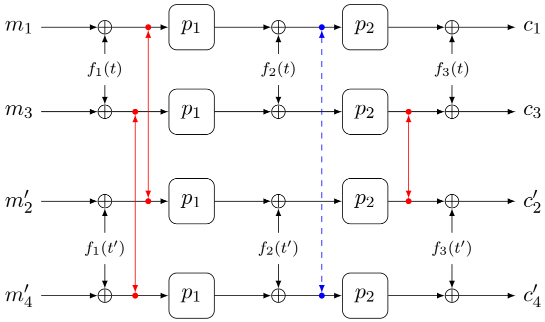
Improved Attack: Rationale



- 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

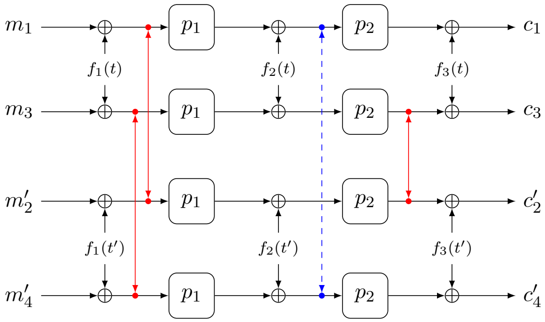


- Stated differently:

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

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

Improved Attack: Rationale

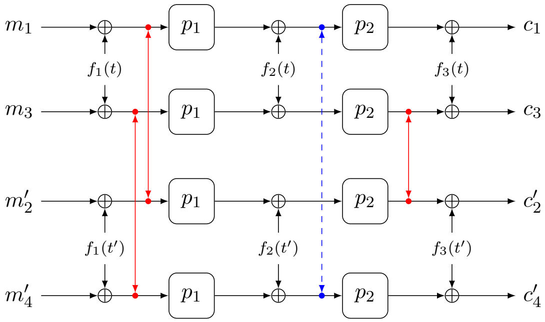


- Stated differently:

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

- 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

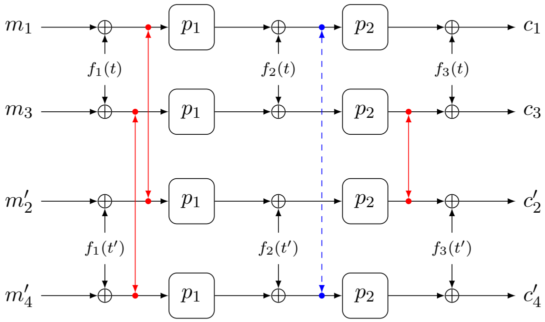


- Stated differently:

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

- 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

Outline

Tweakable Blockciphers Based on Masking

- Intuition
- State of the Art
- Improved Efficiency

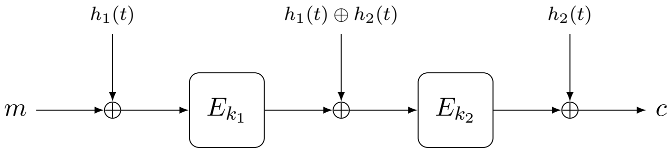
Beyond Birthday Bound Tweakable Blockciphers

- State of the Art
- Tight Security of Cascaded LRW_2?
- Improved Attack
- Improved Security Bound

Conclusion

Improved Security Bound

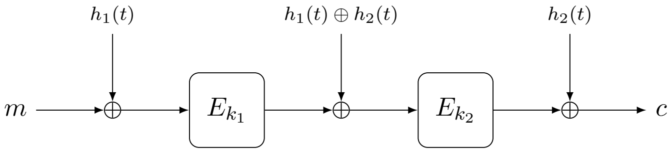
- Cascaded LRW$_2$:



- 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$_2$:



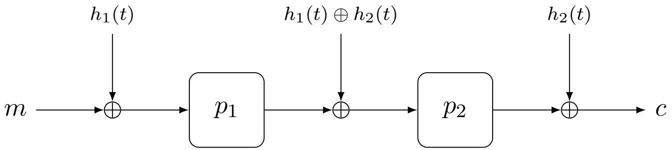
- E_{k_i} are SPRP-secure
- h_i are 4-wise independent XOR-universal hash
- No tweak is queried more than $2^{n/4}$ times

$\boxed{\text{Cascaded LRW}_2 \text{ is secure up to } \approx 2^{3n/4} \text{ evaluations}}$

Improved Security Bound: Proof Idea (1)

Step 1: SPRP Switch

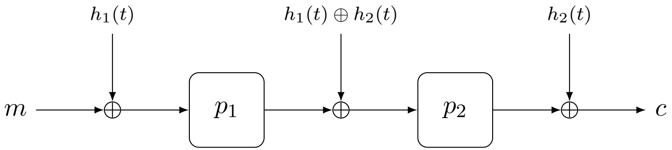
- Replace E_{k_i} by random permutations p_i



Improved Security Bound: Proof Idea (1)

Step 1: SPRP Switch

- Replace E_{k_i} by random permutations p_i

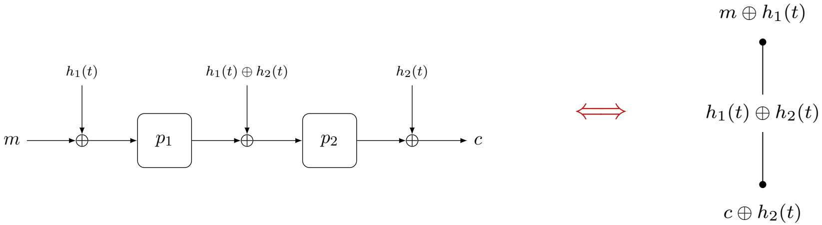


Step 2: Patarin's H-Coefficient Technique

- 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

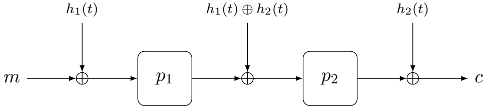
Improved Security Bound: Proof Idea (2)

Step 3: Transform Transcript to Graph (One Tuple)

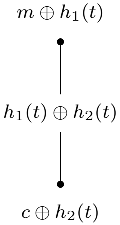


Improved Security Bound: Proof Idea (2)

Step 3: Transform Transcript to Graph (One Tuple)



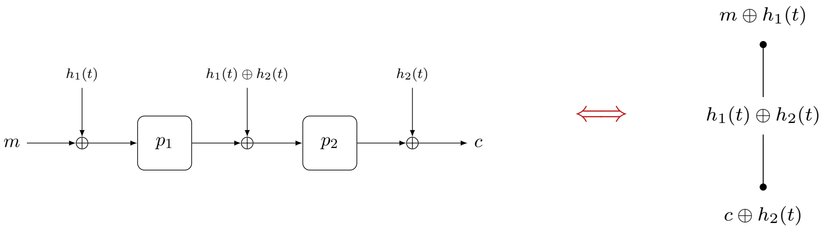
$\Longleftrightarrow$



- 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)

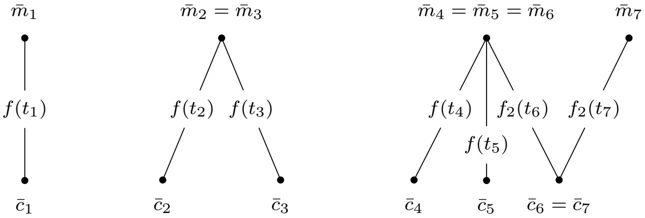
Step 3: Transform Transcript to Graph (One Tuple)



- 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)



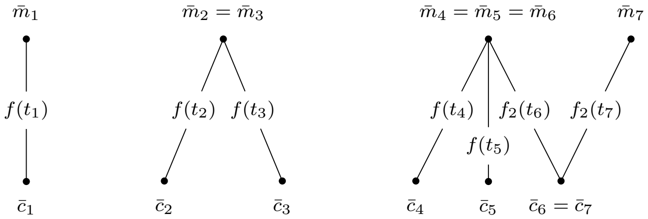
notation:

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

- 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)



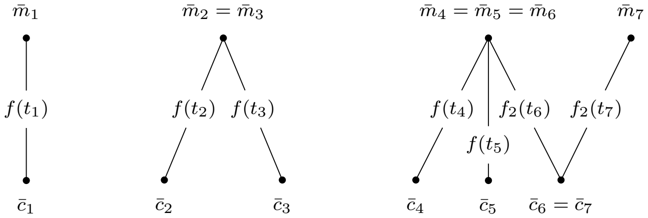
notation:

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

- 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:

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

- 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

Outline

Tweakable Blockciphers Based on Masking

- Intuition
- State of the Art
- Improved Efficiency

Beyond Birthday Bound Tweakable Blockciphers

- State of the Art
- Tight Security of Cascaded LRW_2?
- Improved Attack
- Improved Security Bound

Conclusion

Conclusion

Tweakable Blockciphers: Simple and Powerful

- Myriad applications to AE, MAC, encryption, . . .
- Trade-off between security and efficiency
- Beyond birthday bound security achieved using
  - Extra randomness
  - Extra state size

Conclusion

Tweakable Blockciphers: Simple and Powerful

- Myriad applications to AE, MAC, encryption, ...
- Trade-off between security and efficiency
- Beyond birthday bound security achieved using
  - Extra randomness
  - Extra state size

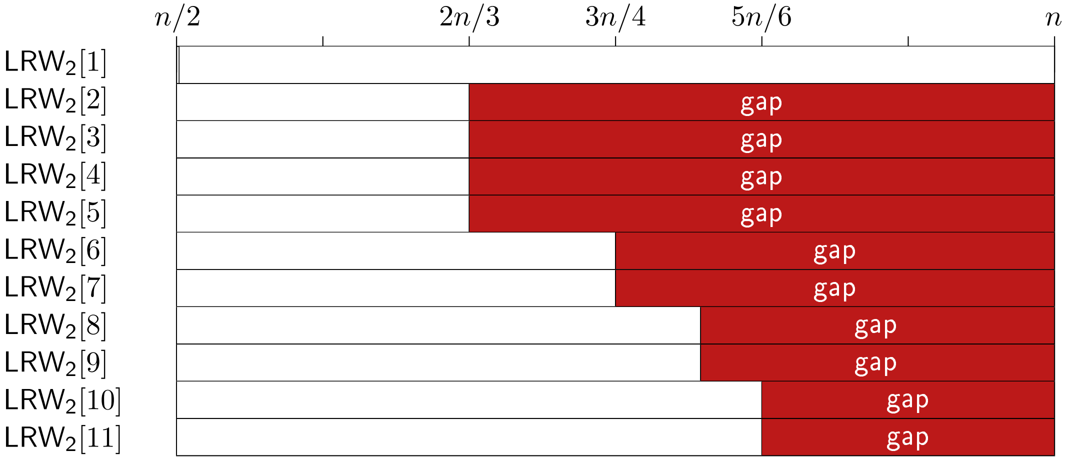
Challenges

- Tightness of cascaded LRW_2 without side conditions?
- Longer cascades of $\mathsf{LRW}_2[\rho]$ and $\mathsf{TEM}[\rho]$?
- Many further open problems in BBB security

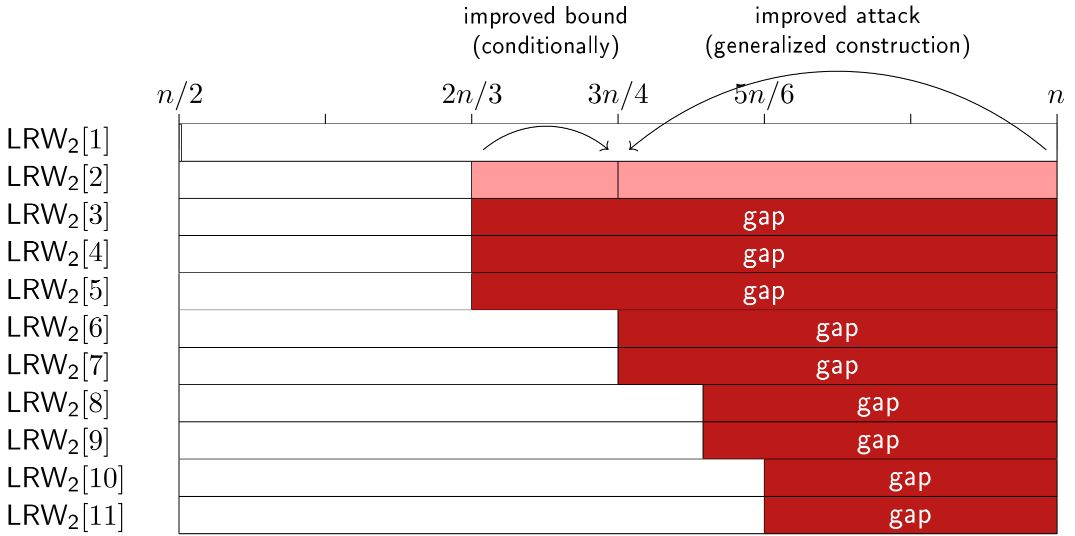
Thank you for your attention!

SUPPORTING SLIDES

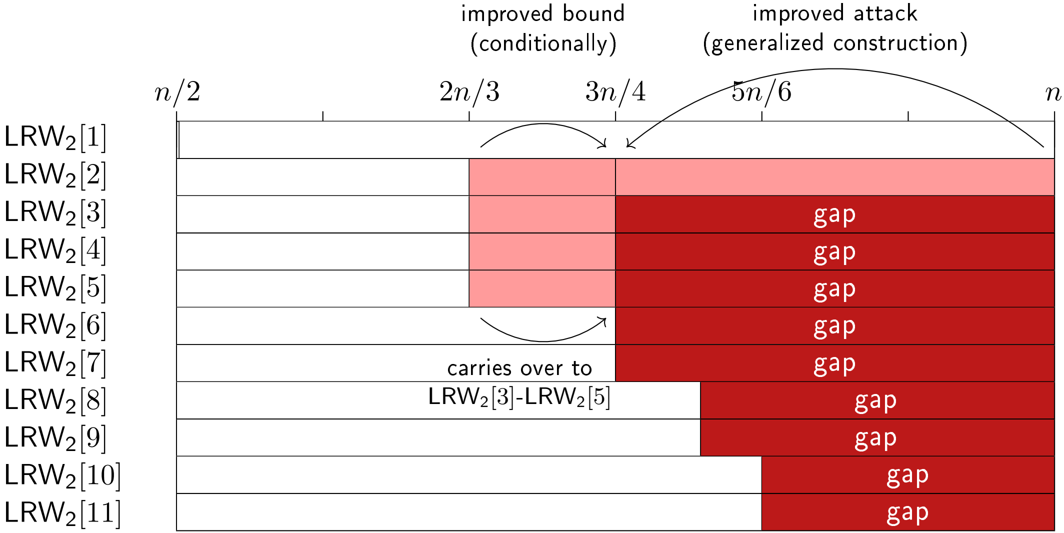
Updated State of the Art on $\mathsf{LRW}_2[\rho]$



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



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

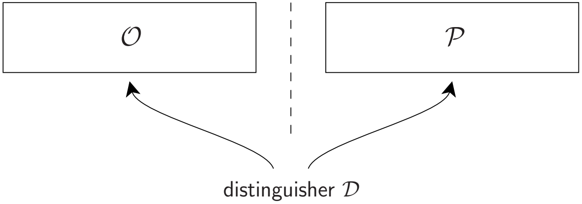


H-Coefficient Technique

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

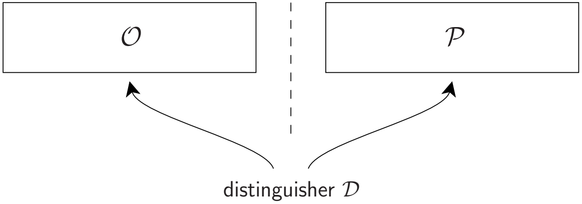
H-Coefficient Technique

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



H-Coefficient Technique

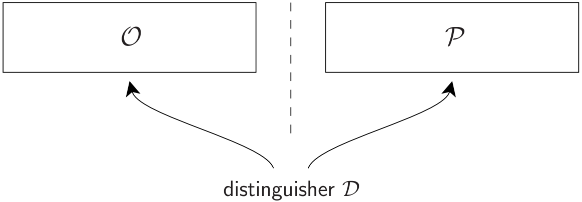
- Patarin [Pat91,Pat08]
- Popularized by Chen and Steinberger [CS14]
- Similar to "Strong Interpolation Technique" [Ber05]



- Basic idea:
  - Each conversation defines a transcript τ

H-Coefficient Technique

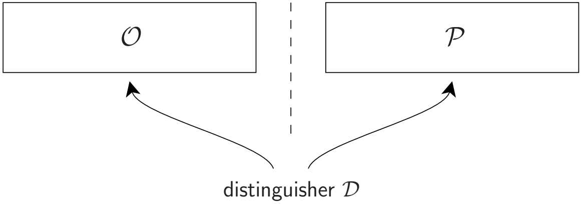
- Patarin [Pat91,Pat08]
- Popularized by Chen and Steinberger [CS14]
- Similar to "Strong Interpolation Technique" [Ber05]



- 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	

Mirror Theory

Patarin's Result

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

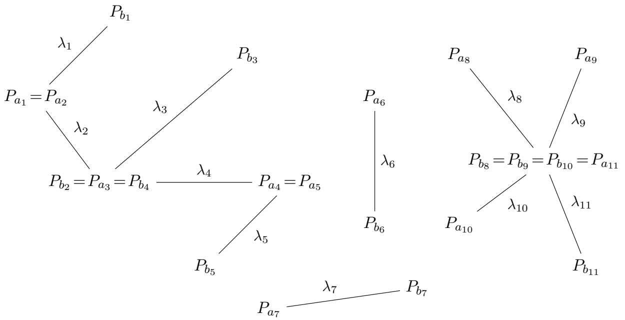
Authors	Publication	Application	Mirror Bound
Patarin	CRYPTO 2003	Feistel	Suboptimal
Patarin	CRYPTO 2004	Feistel	
Patarin	ICISC 2005	Feistel	Optimal in $\mathcal{O}(\cdot)$
Patarin, Montreuil	ICISC 2005	Benes	
Patarin	ICITS 2008	XoP	
Patarin	AFRICACRYPT 2008	Benes	
Patarin	ePrint 2010/287	XoP	Concrete 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	
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 $\varphi : \{a_1, b_1, \ldots, a_q, b_q\} \to \{1, \ldots, r\}$

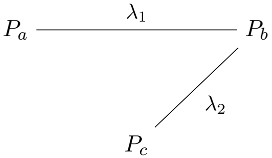
Graph Based View



Mirror Theory: Toy Example 1

- System of equations:

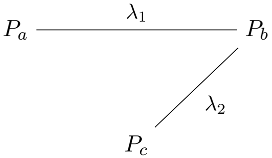
$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$



Mirror Theory: Toy Example 1

- System of equations:

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



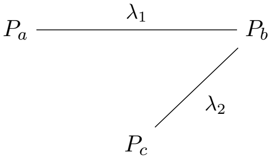
If $\lambda_1 = 0$ or $\lambda_2 = 0$ or $\lambda_1 = \lambda_2$

- 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

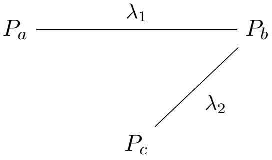
If $\lambda_1, \lambda_2 \neq 0$ and $\lambda_1 \neq \lambda_2$

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

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

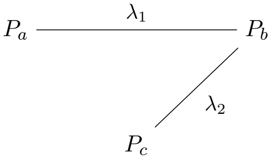
If $\boldsymbol{\lambda_1, \lambda_2 \neq 0}$ and $\boldsymbol{\lambda_1 \neq \lambda_2}$

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

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

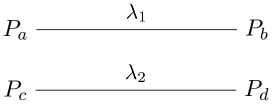
If $\boldsymbol{\lambda_1, \lambda_2 \neq 0}$ and $\boldsymbol{\lambda_1 \neq \lambda_2}$

- 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:

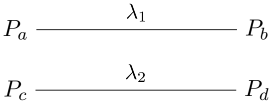
$$P_a \oplus P_b = \lambda_1$$
$$P_c \oplus P_d = \lambda_2$$



Mirror Theory: Toy Example 2

- System of equations:

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



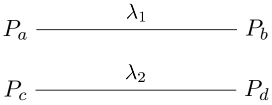
If $\boldsymbol{\lambda_1 = 0}$ or $\boldsymbol{\lambda_2 = 0}$

- 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 $\lambda_1 = 0$ or $\lambda_2 = 0$

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

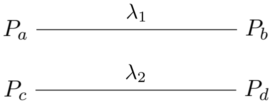
If $\lambda_1, \lambda_2 \neq 0$

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

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

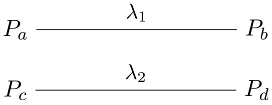
If $\lambda_1, \lambda_2 \neq 0$

- 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 $\lambda_1, \lambda_2 \neq 0$

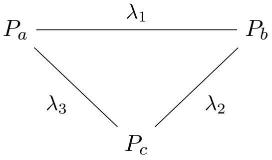
- 2^n choices for P_a (which fixes P_b)
- For P_c and P_d we require
  - $P_c \neq P_a, P_b$
  - $P_d = \lambda_2 \oplus P_c \neq P_a, P_b$
- At least $2^n - 4$ choices for P_c (which fixes P_d)

Mirror Theory: Toy Example 3

- System of equations:

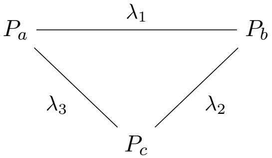
$$P_a \oplus P_b = \lambda_1$$
$$P_b \oplus P_c = \lambda_2$$
$$P_c \oplus P_a = \lambda_3$$

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

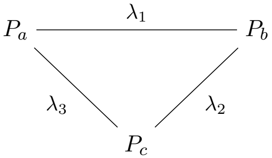
- Contradiction: equations sum to $0 = \lambda_1 \oplus \lambda_2 \oplus \lambda_3$
- Scheme contains a circle

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 $\lambda_1 \oplus \lambda_2 \oplus \lambda_3 \neq 0$

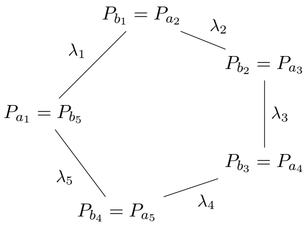
- Contradiction: equations sum to $0 = \lambda_1 \oplus \lambda_2 \oplus \lambda_3$
- Scheme contains a circle

If $\lambda_1 \oplus \lambda_2 \oplus \lambda_3 = 0$

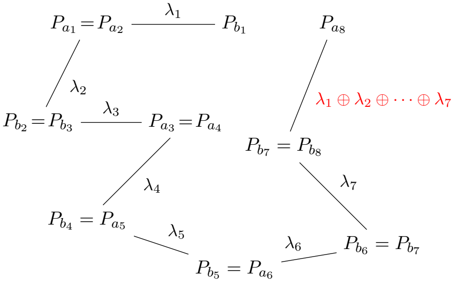
- One redundant equation, no contradiction
- Still counted as circle

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

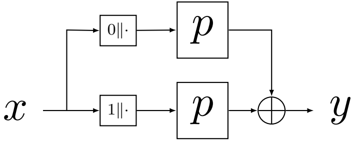
Main Result

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 $(\xi - 1)^2 \cdot r \leq 2^n/67$

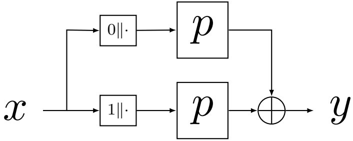
Mirror Theory Applied to XoP



General Setting

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

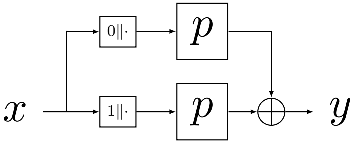
Mirror Theory Applied to XoP



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
  $x_i \mapsto p(1\|x_i) =: P_{b_i}$

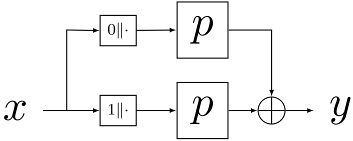
Mirror Theory Applied to XoP



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

$$
\begin{tikzcd}[row sep=large]
P_{a_1} \arrow[d, dash, "y_1"] & P_{a_2} \arrow[d, dash, "y_2"] & \cdots & P_{a_q} \arrow[d, dash, "y_q"] \\
P_{b_1} & P_{b_2} & & P_{b_q}
\end{tikzcd}
$$

Mirror Theory Applied to XoP

$$
\begin{tikzcd}
P_{a_1} \arrow[d, dash, "y_1"] & P_{a_2} \arrow[d, dash, "y_2"] & \cdots & P_{a_q} \arrow[d, dash, "y_q"] \\
P_{b_1} & P_{b_2} & & P_{b_q}
\end{tikzcd}
$$

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

$$\begin{tikzcd} P_{a_1} \arrow[d, dash, "y_1"] & P_{a_2} \arrow[d, dash, "y_2"] & \cdots & P_{a_q} \arrow[d, dash, "y_q"] \\ P_{b_1} & P_{b_2} & & P_{b_q} \end{tikzcd}$$

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:

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

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

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

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

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

$\Big\}\ \varepsilon = 0$

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

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

  $\Big\}\ \varepsilon = 0$

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

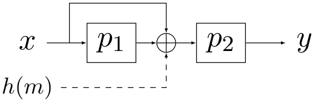
New Look at Mirror Theory

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