Towards Tight Security of Cascaded LRW2

Bart Mennink
Radboud University (The Netherlands)

Theory of Cryptography Conference 2018
November 13, 2018
Tweakable Blockciphers

Diagram:

- $m$ entered into $E$ with key $k$ produces $c$.
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 $\tilde{E}$
  - Tweak $(N,\text{index})$ 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 $\tilde{E}$
    • Tweak $(N, \text{index})$ is unique for every evaluation
    • Different blocks always transformed under different tweak
  • Security of mode often dictated by that of $\tilde{E}$
Tweakable Blockcipher Security

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

\[
\text{Adv}^{\text{stprp}}_{\tilde{E}_k}(D) = \left| \Pr[D \tilde{E}_k, \tilde{E}_k^{-1}] - \Pr[D \tilde{p}, \tilde{p}^{-1}] \right|
\]
Tweakable Blockcipher Security

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

\[
\text{Adv}_{\tilde{E}}^{\text{stprr}}(\mathcal{D}) = \left| \Pr \left[ \mathcal{D}^{\tilde{E}_k, \tilde{E}_k^{-1}} = 1 \right] - \Pr \left[ \mathcal{D}^{\tilde{\pi}, \tilde{\pi}^{-1}} = 1 \right] \right|
\]
Original Constructions

- LRW₁ and LRW₂ 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

- LRW$_2[\rho]$: concatenation of $\rho$ LRW$_2$’s
- $k_1, \ldots, k_\rho$ and $h_1, \ldots, h_\rho$ independent

\[ E_{k_1} \oplus E_{k_2} \oplus \cdots \oplus E_{k_\rho} \]

• Concatenation of $\rho$ LRW$_2$’s
• $k_1, \ldots, k_\rho$ and $h_1, \ldots, h_\rho$ independent
Cascading LRW$_2$’s

$\begin{align*}
\text{LRW}_2[\rho] & : \text{concatenation of } \rho \text{ LRW}_2\text{'s} \\
& = LRW_2[2] \\
\text{k}_1, \ldots, \text{k}_\rho \text{ and } \text{h}_1, \ldots, \text{h}_\rho \text{ independent} \\
\rho = 2 & : \text{secure up to } 2^{2n/3} \text{ queries [LST12,Pro14]} \\
\rho \geq 2 \text{ even} & : \text{secure up to } 2^{\rho n/(\rho+2)} \text{ queries [LS13]} \\
\text{Best attack} & : 2^n \text{ queries}
\end{align*}$
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[ρ]: concatenation of ρ TEM’s
- P₁, ..., Pₖ and h₁, ..., hₖ independent

- ρ = 2: secure up to $2^{2n/3}$ queries [CLS15]
- ρ ≥ 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

LRW$_2$[1]
LRW$_2$[2]
LRW$_2$[3]
LRW$_2$[4]
LRW$_2$[5]
LRW$_2$[6]
LRW$_2$[7]
LRW$_2$[8]
LRW$_2$[9]
LRW$_2$[10]
LRW$_2$[11]

TEM[1]
TEM[2]
TEM[3]
TEM[4]
TEM[5]
TEM[6]
TEM[7]
TEM[8]
TEM[9]
TEM[10]
TEM[11]
Tight Security of Cascaded LRW2?

\[ m \oplus h_1(t) \rightarrow E_{k_1} \oplus h_1(t) \oplus h_2(t) \rightarrow E_{k_2} \oplus h_2(t) \rightarrow c \]
Tight Security of Cascaded LRW$_2$?
Tight Security of Cascaded LRW$_2$?

\[
m \oplus h_1(t) \rightarrow E_{k_1} \oplus h_1(t) \oplus h_2(t) \rightarrow E_{k_2} \oplus h_2(t) \rightarrow c
\]

Improved bound (conditionally)

Improved attack (generalized construction)

n/2 \quad 2n/3 \quad 3n/4 \quad n
Tight Security of Cascaded LRW$_2$?

\[
m \oplus h_1(t) \rightarrow E_{k_1} \oplus h_1(t) \oplus h_2(t) \rightarrow E_{k_2} \oplus h_2(t) \rightarrow c
\]

\[
m/2 \rightarrow 2n/3 \rightarrow 3n/4 \rightarrow n
\]

improved bound (conditionally)

improved attack (generalized construction)

Improved Attack

- GCL (Generalized Cascaded LRW$_2$):

\[ m \rightarrow E_{k_1} \rightarrow E_{k_2} \rightarrow c \]

\( f_1(t) \)
\( f_2(t) \)
\( f_3(t) \)

- \( f_i \) are arbitrary functions
- \( p_i := E_{k_i} \) are random permutations
Improved Attack

- GCL (Generalized Cascaded LRW$_2$):

\[ m \oplus E_{k_1} \oplus E_{k_2} \oplus c \]

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

**Generic distinguishing attack in $2^{n^{1/2}}2^{3n/4}$ evaluations**
• 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 $D$ 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 $D$ 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 \( D \) 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 \( D \) 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 \( t' \))

- \( \mathbb{E}[\text{solutions to } c'_2 \oplus c_3 = c_1 \oplus c'_4]? \)
  - 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 \( t' \))

• \( \mathbb{E}[\text{solutions to } c'_2 \oplus c_3 = c_1 \oplus c'_4] \)?
  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 $D$ is at least $1/2$
- Analysis consists of properly bounding $\Pr[D \tilde{E}_k = 1]$ and $\Pr[D \tilde{\pi} = 1]$
### 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 $\Pr[\mathcal{D} \tilde{E}_k = 1]$ and $\Pr[\mathcal{D} \tilde{\pi} = 1]$

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

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

- Cascaded LRW$_2$:

\[
\begin{align*}
  m & \oplus h_1(t) \rightarrow E_{k_1} \oplus h_1(t) \oplus h_2(t) \rightarrow E_{k_2} \oplus h_2(t) \\
  & \rightarrow c
\end{align*}
\]

- $E_{k_i}$ 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$_2$:

\[ m \oplus E_{k_1} \oplus E_{k_2} \oplus h_1(t) \oplus h_2(t) = c \]

- $E_{k_i}$ 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
Step 1: SPRP Switch

- Replace $E_{k_i}$ by random permutations $p_i$

![Diagram](image)
**Improved Security Bound: Proof Idea (1)**

**Step 1: SPRP Switch**
- Replace $E_{k_i}$ by random permutations $p_i$

![Diagram](image)

**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)**

\[
\begin{align*}
m \oplus h_1(t) &\iff m \oplus h_1(t) \\
h_1(t) \oplus h_2(t) &\iff h_1(t) \oplus h_2(t) \\
c \oplus h_2(t) &\iff c \oplus h_2(t)
\end{align*}
\]
Improving 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: \( X \oplus Y = h_1(t) \oplus h_2(t) \)
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 $(X, Y)$
Step 4: Transform Transcript to Graph (All Tuples)

- \( \bar{m}_1 = m_1 \oplus h_1(t_i) \)
- \( \bar{c}_1 = c_i \oplus h_2(t_i) \)
- \( f(t_i) = h_1(t_i) \oplus h_2(t_i) \)

- \( r_1 \) 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)**

\[
\begin{align*}
\bar{m}_1  & \quad \bar{m}_2 = \bar{m}_3  \\
\bar{c}_1  & \quad \bar{c}_2  \\
\bar{c}_1  & \quad \bar{c}_2  \\
\bar{c}_1  & \quad \bar{c}_2  \\
\bar{c}_1  & \quad \bar{c}_2  \\
\end{align*}
\]

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

\[
\begin{align*}
\bar{m}_4 = \bar{m}_5 = \bar{m}_6  & \quad \bar{m}_7  \\
\bar{c}_4  & \quad \bar{c}_5  \\
\bar{c}_4  & \quad \bar{c}_5  \\
\bar{c}_4  & \quad \bar{c}_5  \\
\bar{c}_4  & \quad \bar{c}_5  \\
\end{align*}
\]

notation:
\[
\begin{align*}
\bar{m}_i &= m_i \oplus h_1(t_i) \\
\bar{c}_i &= c_i \oplus h_2(t_i) \\
f(t_i) &= h_1(t_i) \oplus h_2(t_i)
\end{align*}
\]
Step 4: Transform Transcript to Graph (All Tuples)

- $r_1$ 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
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

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

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

- 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 \(O(q^4/2^{3n})\)
**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 LRW₂ (or LRW₂[2])

- Generic attack in complexity $3n/4$
- $3n/4$ security bound, but conditional
- Security bound carries over to LRW₂[3]–LRW₂[5]
Conclusion

Cascaded LRW$_2$ (or LRW$_2[2]$)

- Generic attack in complexity $3n/4$
- $3n/4$ security bound, but conditional

Challenges

- Tightness of cascaded LRW$_2$ without side conditions?
- Longer cascades of LRW$_2[\rho]$ and TEM[\rho]?

Thank you for your attention!
Updated State of the Art on $\text{LRW}_2[\rho]$

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$n/2$</td>
<td>2$n/3$</td>
<td>3$n/4$</td>
<td>5$n/6$</td>
<td>$n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>gap</td>
<td>gap</td>
<td>gap</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Updated State of the Art on LRW$_2[\rho]$

- LRW$_2[1]$
- LRW$_2[2]$
- LRW$_2[3]$
- LRW$_2[4]$
- LRW$_2[5]$
- LRW$_2[6]$
- LRW$_2[7]$
- LRW$_2[8]$
- LRW$_2[9]$
- LRW$_2[10]$
- LRW$_2[11]$

- Improved bound (conditionally)
- Improved attack (generalized construction)

- LRW$_2[6]$
- LRW$_2[7]$
- LRW$_2[8]$
- LRW$_2[9]$
- LRW$_2[10]$
- LRW$_2[11]$
Updated State of the Art on $\text{LRW}_2[\rho]$

![Diagram showing the state of the art on $\text{LRW}_2[\rho]$ with improved bounds and attacks.](image)

- **Improved Bound (conditionally):**
  - $n/2$
  - $2n/3$
  - $3n/4$
  - $5n/6$
  - $n$

- **Improved Attack (generalized construction):**
  - $n/2$
  - $2n/3$
  - $3n/4$
  - $5n/6$
  - $n$

- **Gaps:**
  - $\text{LRW}_2[1]$
  - $\text{LRW}_2[2]$
  - $\text{LRW}_2[3]$
  - $\text{LRW}_2[4]$
  - $\text{LRW}_2[5]$
  - $\text{LRW}_2[6]$
  - $\text{LRW}_2[7]$
  - $\text{LRW}_2[8]$
  - $\text{LRW}_2[9]$
  - $\text{LRW}_2[10]$
  - $\text{LRW}_2[11]$

- **Carries Over To:**
  - $\text{LRW}_2[3]-\text{LRW}_2[5]$
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]

![Diagram showing O and P boxes with distinguisher D arrowed between them.]

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

Lemma
Let $\epsilon \geq 0$ be such that for all good transcripts $\tau$:

$$\Pr[O \text{ gives } \tau] \geq 1 - \epsilon$$

Then,

$$\Delta \mathcal{D}(O; P) \leq \epsilon + \Pr[\text{bad transcript for } P]$$

Trade-off: define bad transcripts smartly!
H-Coefficient Technique

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

\[ \text{Lemma} \]
Let $\varepsilon \geq 0$ be such that for all good transcripts $\tau$:
\[
\Pr[O \text{ gives } \tau] - \Pr[P \text{ gives } \tau] \geq 1 - \varepsilon
\]
Then,
\[
\Delta_D(O; P) \leq \varepsilon + \Pr[\text{bad transcript for } P]
\]
Trade-off: define bad transcripts smartly!
H-Coefficient Technique

• \( \mathcal{D} \) is computationally unbounded and deterministic
• Each conversation defines a transcript \( \tau \)
• Consider good and bad transcripts

**Lemma**

Let \( \varepsilon \geq 0 \) be such that for all good transcripts \( \tau \):

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

Then, \( \Delta_D(\mathcal{O}; P) \leq \varepsilon + \Pr[\text{bad transcript for } \mathcal{P}] \)
H-Coefficient Technique

- $D$ is computationally unbounded and deterministic
- Each conversation defines a transcript $\tau$
- Consider good and bad transcripts

Lemma
Let $\epsilon \geq 0$ be such that for all good transcripts $\tau$:

\[
\frac{\Pr[\mathcal{O} \text{ gives } \tau]}{\Pr[\mathcal{P} \text{ gives } \tau]} \geq 1 - \epsilon
\]

Then, $\Delta_D(\mathcal{O}; P) \leq \epsilon + \Pr[\text{bad transcript for } \mathcal{P}]$

Trade-off: define bad transcripts smartly!
System of Equations

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

\[
\begin{align*}
P_{a_1} \oplus P_{b_1} &= \lambda_1 \\
P_{a_2} \oplus P_{b_2} &= \lambda_2 \\
&\vdots \\
P_{a_q} \oplus P_{b_q} &= \lambda_q
\end{align*}
\]

for some surjection \( \varphi : \{a_1, b_1, \ldots, a_q, b_q\} \rightarrow \{1, \ldots, r\} \)
System of Equations

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

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

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)

<table>
<thead>
<tr>
<th>Authors</th>
<th>Publication</th>
<th>Application</th>
<th>Mirror Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patarin</td>
<td>CRYPTO 2003</td>
<td>Feistel</td>
<td>Suboptimal</td>
</tr>
</tbody>
</table>
## Patarin’s Result

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

<table>
<thead>
<tr>
<th>Authors</th>
<th>Publication</th>
<th>Application</th>
<th>Mirror Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patarin</td>
<td>CRYPTO 2003</td>
<td>Feistel</td>
<td>Suboptimal</td>
</tr>
<tr>
<td>Patarin</td>
<td>CRYPTO 2004</td>
<td>Feistel</td>
<td></td>
</tr>
</tbody>
</table>
Mirror Theory

Patarin’s Result

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

<table>
<thead>
<tr>
<th>Authors</th>
<th>Publication</th>
<th>Application</th>
<th>Mirror Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patarin</td>
<td>CRYPTO 2003</td>
<td>Feistel</td>
<td>Suboptimal</td>
</tr>
<tr>
<td>Patarin</td>
<td>CRYPTO 2004</td>
<td>Feistel</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ICISC 2005</td>
<td>Feistel</td>
<td>Optimal in $O(\cdot)$</td>
</tr>
</tbody>
</table>
Mirror Theory

**Patarin’s Result**

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

<table>
<thead>
<tr>
<th>Authors</th>
<th>Publication</th>
<th>Application</th>
<th>Mirror Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patarin</td>
<td>CRYPTO 2003</td>
<td>Feistel</td>
<td>Suboptimal</td>
</tr>
<tr>
<td>Patarin</td>
<td>CRYPTO 2004</td>
<td>Feistel</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ICISC 2005</td>
<td>Feistel</td>
<td>Optimal in $\mathcal{O}(\cdot)$</td>
</tr>
<tr>
<td>Patarin, Montreuil</td>
<td>ICISC 2005</td>
<td>Benes</td>
<td></td>
</tr>
</tbody>
</table>
Mirror Theory

Patarin’s Result

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

<table>
<thead>
<tr>
<th>Authors</th>
<th>Publication</th>
<th>Application</th>
<th>Mirror Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patarin</td>
<td>CRYPTO 2003</td>
<td>Feistel</td>
<td>Suboptimal</td>
</tr>
<tr>
<td>Patarin</td>
<td>CRYPTO 2004</td>
<td>Feistel</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ICISC 2005</td>
<td>Feistel</td>
<td>Optimal in $O(\cdot)$</td>
</tr>
<tr>
<td>Patarin, Montreuil</td>
<td>ICISC 2005</td>
<td>Benes</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ICITS 2008</td>
<td>XoP</td>
<td></td>
</tr>
</tbody>
</table>
Patarin’s Result

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

<table>
<thead>
<tr>
<th>Authors</th>
<th>Publication</th>
<th>Application</th>
<th>Mirror Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patarin</td>
<td>CRYPTO 2003</td>
<td>Feistel</td>
<td>Suboptimal</td>
</tr>
<tr>
<td>Patarin</td>
<td>CRYPTO 2004</td>
<td>Feistel</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ICISC 2005</td>
<td>Feistel</td>
<td>Optimal in $O(\cdot)$</td>
</tr>
<tr>
<td>Patarin, Montreuil</td>
<td>ICISC 2005</td>
<td>Benes</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ICITS 2008</td>
<td>XoP</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>AFRICACRYPT 2008</td>
<td>Benes</td>
<td></td>
</tr>
</tbody>
</table>
Mirror Theory

Patarin’s Result

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

<table>
<thead>
<tr>
<th>Authors</th>
<th>Publication</th>
<th>Application</th>
<th>Mirror Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patarin</td>
<td>CRYPTO 2003</td>
<td>Feistel</td>
<td>Suboptimal</td>
</tr>
<tr>
<td>Patarin</td>
<td>CRYPTO 2004</td>
<td>Feistel</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ICISC 2005</td>
<td>Feistel</td>
<td>Optimal in $O(\cdot)$</td>
</tr>
<tr>
<td>Patarin, Montreuil</td>
<td>ICISC 2005</td>
<td>Benes</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ICITS 2008</td>
<td>XoP</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>AFRICACRYPT 2008</td>
<td>Benes</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ePrint 2010/287</td>
<td>XoP</td>
<td>Concrete bound</td>
</tr>
</tbody>
</table>
Mirror Theory

Patarin’s Result

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

<table>
<thead>
<tr>
<th>Authors</th>
<th>Publication</th>
<th>Application</th>
<th>Mirror Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patarin</td>
<td>CRYPTO 2003</td>
<td>Feistel</td>
<td>Suboptimal</td>
</tr>
<tr>
<td>Patarin</td>
<td>CRYPTO 2004</td>
<td>Feistel</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ICISC 2005</td>
<td>Feistel</td>
<td></td>
</tr>
<tr>
<td>Patarin, Montreuil</td>
<td>ICISC 2005</td>
<td>Benes</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ICITS 2008</td>
<td>XoP</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>AFRICACRYPT 2008</td>
<td>Benes</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ePrint 2010/287</td>
<td>XoP</td>
<td>Concrete bound</td>
</tr>
<tr>
<td>Patarin</td>
<td>ePrint 2010/293</td>
<td>Feistel</td>
<td></td>
</tr>
</tbody>
</table>
**Patarin’s Result**

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

<table>
<thead>
<tr>
<th>Authors</th>
<th>Publication</th>
<th>Application</th>
<th>Mirror Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patarin</td>
<td>CRYPTO 2003</td>
<td>Feistel</td>
<td>Suboptimal</td>
</tr>
<tr>
<td>Patarin</td>
<td>CRYPTO 2004</td>
<td>Feistel</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ICISC 2005</td>
<td>Feistel</td>
<td>Optimal in $\mathcal{O}(\cdot)$</td>
</tr>
<tr>
<td>Patarin, Montreuil</td>
<td>ICISC 2005</td>
<td>Benes</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ICITS 2008</td>
<td>XoP</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>AFRICACRYPT 2008</td>
<td>Benes</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ePrint 2010/287</td>
<td>XoP</td>
<td>Concrete bound</td>
</tr>
<tr>
<td>Patarin</td>
<td>ePrint 2010/293</td>
<td>Feistel</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ePrint 2013/368</td>
<td>XoP</td>
<td></td>
</tr>
</tbody>
</table>
## Patarin’s Result

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

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

Patarin’s Result

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

<table>
<thead>
<tr>
<th>Authors</th>
<th>Publication</th>
<th>Application</th>
<th>Mirror Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patarin</td>
<td>CRYPTO 2003</td>
<td>Feistel</td>
<td>Suboptimal</td>
</tr>
<tr>
<td>Patarin</td>
<td>CRYPTO 2004</td>
<td>Feistel</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ICISC 2005</td>
<td>Feistel</td>
<td>Optimal in $O(\cdot)$</td>
</tr>
<tr>
<td>Patarin, Montreuil</td>
<td>ICISC 2005</td>
<td>Benes</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ICITS 2008</td>
<td>XoP</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>AFRICACRYPT 2008</td>
<td>Benes</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ePrint 2010/287</td>
<td>XoP</td>
<td>Concrete bound</td>
</tr>
<tr>
<td>Patarin</td>
<td>ePrint 2010/293</td>
<td>Feistel</td>
<td></td>
</tr>
<tr>
<td>Patarin</td>
<td>ePrint 2013/368</td>
<td>XoP</td>
<td></td>
</tr>
<tr>
<td>Cogliati, Lampe, Patarin</td>
<td>FSE 2014</td>
<td>XoP\textsuperscript{d}</td>
<td></td>
</tr>
<tr>
<td>Volte, Nachev, Marrière</td>
<td>ePrint 2016/136</td>
<td>Feistel</td>
<td></td>
</tr>
</tbody>
</table>
Mirror Theory

**Patarin’s Result**

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

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

System of Equations

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

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:
  \[
  \begin{align*}
  P_a \oplus P_b &= \lambda_1 \\
  P_b \oplus P_c &= \lambda_2
  \end{align*}
  \]

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 \( \lambda_1 = 0 \) 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 \( \lambda_1 \oplus \lambda_2 \oplus \lambda_3 \neq 0 \)

- 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**

\[ P_{b1} = P_{a2} \]
\[ \lambda_1 \]
\[ P_{a1} = P_{b5} \]
\[ \lambda_5 \]
\[ P_{b4} = P_{a5} \]
\[ \lambda_4 \]
\[ P_{b3} = P_{a4} \]

\[ P_{b2} = P_{a3} \]
\[ \lambda_2 \]

**Degeneracy**

\[ P_{a1} = P_{a2} \]
\[ \lambda_1 \]
\[ P_{b1} \]
\[ \lambda_2 \]
\[ P_{b2} = P_{a3} \]
\[ \lambda_3 \]
\[ P_{a4} \]
\[ \lambda_4 \]
\[ P_{b3} = P_{b4} = P_{a5} \]
\[ \lambda_5 \]
\[ P_{b5} = P_{a6} \]
\[ \lambda_6 \]
\[ P_{b6} = P_{b7} \]
\[ \lambda_7 \]
\[ \lambda_1 \oplus \lambda_2 \oplus \cdots \oplus \lambda_7 \]
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 $\varphi: \{a_1, b_1, \ldots, a_q, b_q\} \rightarrow \{1, \ldots, r\}$

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 $\xi$ satisfies $(\xi - 1)^2 \cdot r \leq 2^n/67$
**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 \( x_i \leftrightarrow p(0||x_i) =: P_{a_i} \) and 
  \[ x_i \leftrightarrow p(1||x_i) =: P_{b_i} \]
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 $x_i \mapsto p(0 \parallel x_i) =: P_{a_i}$ and $x_i \mapsto p(1 \parallel x_i) =: P_{b_i}$
- System of $q$ equations $P_{a_i} \oplus P_{b_i} = y_i$
- Inputs to $p$ are all distinct: $2q$ unknowns
Applying Mirror Theory

- Circle-free: no collisions in inputs to $P$
- Non-degenerate: provided that $y_i \neq 0$ for all $i$

Call this a bad transcript

Maximum tree size $2^{q}$

If $2^{q} \leq \frac{2^n}{67}$: at least $2^{nq}$ solutions to unknowns
Applying Mirror Theory

- **Circle-free**: no collisions in inputs to $p$
- **Non-degenerate**: provided that $y_i \neq 0$ for all $i$
  \[\rightarrow\text{ Call this a bad transcript}\]
- **Maximum tree size** 2
Applying Mirror Theory

- **Circle-free**: no collisions in inputs to $p$
- **Non-degenerate**: provided that $y_i \neq 0$ for all $i$
  $\rightarrow$ 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
H-Coefficient Technique [Pat91,Pat08,CS14]

Let \( \varepsilon \geq 0 \) be such that for all good transcripts \( \tau \):

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

Then, \( \text{Adv}^{\text{prf}}_{XoP}(q) \leq \varepsilon + \Pr[\text{bad transcript for } f] \)
**H-Coefficient Technique** [Pat91,Pat08,CS14]

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

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

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

- **Bad transcript**: if $y_i = 0$ for some $i$
  - $\Pr[\text{bad transcript for } f] = q/2^n$
Mirror Theory Applied to XoP

**H-Coefficient Technique** [Pat91,Pat08,CS14]

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

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

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

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

**H-Coefficient Technique [Pat91,Pat08,CS14]**

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

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

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

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

**H-Coefficient Technique [Pat91,Pat08,CS14]**

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

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

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

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

- **For any good transcript**:
  - $\Pr[\text{XoP gives } \tau] \geq \frac{(2^n)_{2q}}{2^{nq}} \cdot \frac{1}{(2^n)_{2q}}$
  - $\Pr[\text{f gives } \tau] = \frac{1}{2^{nq}}$

\[\varepsilon = 0\]
Mirror Theory Applied to XoP

**H-Coefficient Technique [Pat91,Pat08,CS14]**

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

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

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

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

  $$\text{Adv}^\text{prf}_{\text{XoP}}(q) \leq q/2^n$$
New Look at Mirror Theory

Mennink, Neves, CRYPTO 2017

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

E(WC)DM [CS16]

```
x --- p1 --> p2 --> y
h(m)--------
```

EDMD

```
x --- p1 --> p2 --> y
```