Fine-Tuning Ideal Worlds for the Xor of Two Permutation Outputs

Wonseok Choi[1] Minki Hhan[2] Yu Wei[1] Vassilis Zikas[1]

[1]Purdue University, West Lafayette, IN, USA

[2]Korea Institute for Advanced Study, Seoul, Korea

December 3rd, 2023

Outline

Luby-Rackoff Problem

- Feistel and Coppersmith: designed IBM's Lucifer cipher using Feistel networks
- Luby and Rackoff: analyzed Feistel network when the round function is a secure pseudorandom function (PRF)
  - 3 rounds: a pseudorandom permutation (PRP),
  - 4 rounds: a strong pseudorandom permutation
- Luby-Rackoff problem: how to make secure PRPs from secure PRFs?

Luby-Rackoff Problem

- Feistel and Coppersmith: designed IBM's Lucifer cipher using Feistel networks
- Luby and Rackoff: analyzed Feistel network when the round function is a secure pseudorandom function (PRF)
  - 3 rounds: a pseudorandom permutation (PRP),
  - 4 rounds: a strong pseudorandom permutation
- Luby-Rackoff problem: how to make secure PRPs from secure PRFs?

Luby-Rackoff Problem

- Feistel and Coppersmith: designed IBM's Lucifer cipher using Feistel networks
- Luby and Rackoff: analyzed Feistel network when the round function is a secure pseudorandom function (PRF)
  - 3 rounds: a pseudorandom permutation (PRP),
  - 4 rounds: a strong pseudorandom permutation
- Luby-Rackoff problem: how to make secure PRPs from secure PRFs?

Luby-Rackoff Backward Problem

- AES is everywhere nowadays
  - AES, or any other block ciphers, is typically modeled as a PRP
- Meanwhile, hashes, message authenticate codes (MACs), or authenticated encryptions (AEs or AEADs) prefer to use PRFs — at least implicitly in their security proofs!
- Luby-Rackoff backward problem: how to make secure PRFs from secure PRPs?

Luby-Rackoff Backward Problem

- AES is everywhere nowadays
  - AES, or any other block ciphers, is typically modeled as a PRP
- Meanwhile, hashes, message authenticate codes (MACs), or authenticated encryptions (AEs or AEADs) prefer to use PRFs — at least implicitly in their security proofs!
- Luby-Rackoff backward problem: how to make secure PRFs from secure PRPs?

Luby-Rackoff Backward Problem

- AES is everywhere nowadays
  - AES, or any other block ciphers, is typically modeled as a PRP
- Meanwhile, hashes, message authenticate codes (MACs), or authenticated encryptions (AEs or AEADs) prefer to use PRFs — at least implicitly in their security proofs!
- Luby-Rackoff backward problem: how to make secure PRFs from secure PRPs?

XoP1 and XoP2

- How to build secure PRFs from secure PRPs?

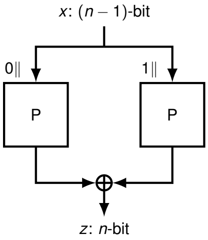


Figure 1: XoP1 based on a single (keyed) PRP: P

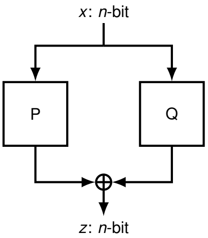


Figure 2: XoP2 based on two (keyed) PRPs: P and Q

Applications

- Symmetric-key primitive designs to achieve beyond birthday-bound (BBB) security
- MACs: nEHtM [DNT19], DbHtS [DDNP18], EWCDM [CS16]
- AEADs: CWC+ [DNT19], SCM [CLLL21], XOCB [BH+23]

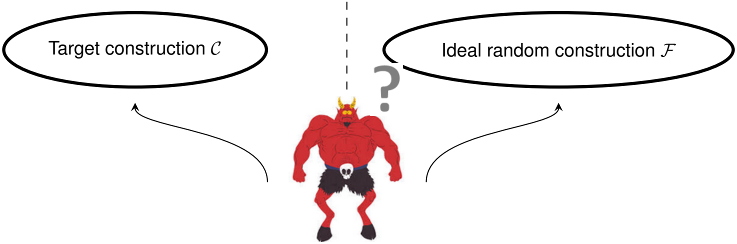
Applications

- Symmetric-key primitive designs to achieve beyond birthday-bound (BBB) security
- MACs: nEHtM [DNT19], DbHtS [DDNP18], EWCDM [CS16]
- AEADs: CWC+ [DNT19], SCM [CLLL21], XOCB [BH+23]

Applications

- Symmetric-key primitive designs to achieve beyond birthday-bound (BBB) security
- MACs: nEHtM [DNT19], DbHtS [DDNP18], EWCDM [CS16]
- AEADs: CWC+ [DNT19], SCM [CLLL21], XOCB [BH+23]

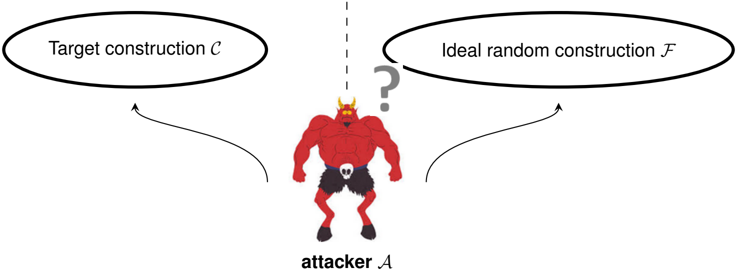
Security Notion: Single-User PRF Security



attacker $\mathcal{A}$

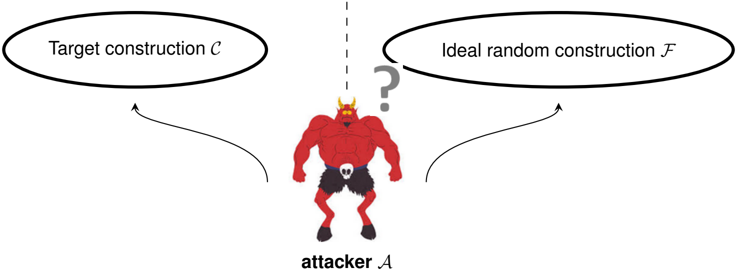
- $\mathcal{A}$ makes q queries to the construction oracle ($\mathcal{C}$ or $\mathcal{F}$)
- Security: a distinguishing probability of the two worlds:
  - $\mathbf{Adv}^{\mathrm{su}}_{\mathcal{C}}(\mathcal{A})$ can be denoted as a function of q
- $\mathbf{Adv}^{\mathrm{su}}_{\mathcal{C}}(\mathcal{A})$ is negligible $\Longrightarrow$ $\mathcal{C}$ is secure

Security Notion: Single-User PRF Security



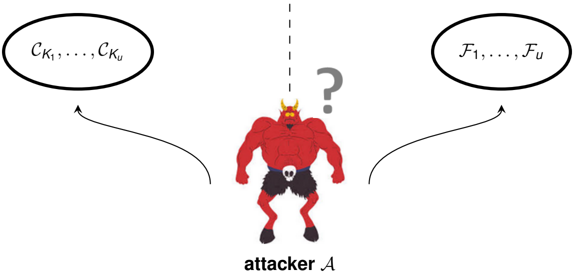
- $\mathcal{A}$ makes q queries to the construction oracle ($\mathcal{C}$ or $\mathcal{F}$)
- Security: a distinguishing probability of the two worlds:
  - $\mathbf{Adv}_{\mathcal{C}}^{\mathrm{su}}(\mathcal{A})$ can be denoted as a function of q
- $\mathbf{Adv}_{\mathcal{C}}^{\mathrm{su}}(\mathcal{A})$ is negligible $\Longrightarrow$ $\mathcal{C}$ is secure

Security Notion: Single-User PRF Security



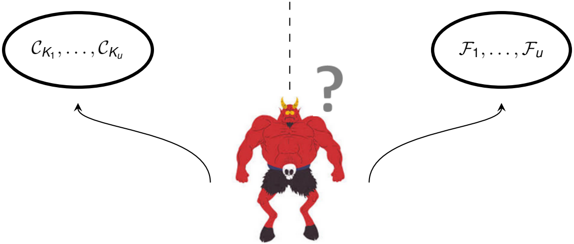
- $\mathcal{A}$ makes q queries to the construction oracle ($\mathcal{C}$ or $\mathcal{F}$)
- Security: a distinguishing probability of the two worlds:
  - $\mathbf{Adv}^{\mathsf{su}}_{\mathcal{C}}(\mathcal{A})$ can be denoted as a function of q
- $\mathbf{Adv}^{\mathsf{su}}_{\mathcal{C}}(\mathcal{A})$ is negligible $\Longrightarrow$ $\mathcal{C}$ is secure

Security Notion: Multi-User PRF Security



- $\mathcal{A}$ makes q queries to u construction oracles ($\mathcal{C}_{K_1}, \ldots, \mathcal{C}_{K_u}$ or $\mathcal{F}_1, \ldots, \mathcal{F}_u$)
- $\mathcal{A}$ succeeds as long as it can compromise K_i for any i
- Naive hybrid argument $\mathbf{Adv}^{\mathrm{mu}}_{\mathcal{C}}(\mathcal{A}) = u \cdot \mathbf{Adv}^{\mathrm{su}}_{\mathcal{C}}(\mathcal{A})$

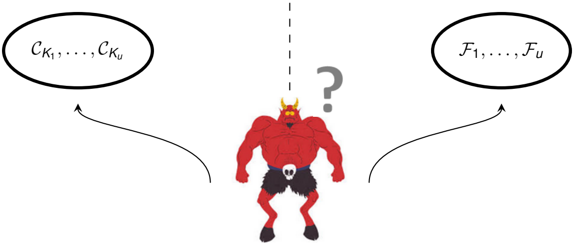
Security Notion: Multi-User PRF Security



attacker $\mathcal{A}$

- $\mathcal{A}$ makes q queries to u construction oracles ($\mathcal{C}_{K_1}, \ldots, \mathcal{C}_{K_u}$ or $\mathcal{F}_1, \ldots, \mathcal{F}_u$)
- $\mathcal{A}$ succeeds as long as it can compromise K_i for any i
- Naive hybrid argument $\mathbf{Adv}_{\mathcal{C}}^{\mathrm{mu}}(\mathcal{A}) = u \cdot \mathbf{Adv}_{\mathcal{C}}^{\mathrm{su}}(\mathcal{A})$

Security Notion: Multi-User PRF Security



attacker $\mathcal{A}$

- $\mathcal{A}$ makes q queries to u construction oracles ($\mathcal{C}_{K_1}, \ldots, \mathcal{C}_{K_u}$ or $\mathcal{F}_1, \ldots, \mathcal{F}_u$)
- $\mathcal{A}$ succeeds as long as it can compromise K_i for any i
- Naive hybrid argument $\mathbf{Adv}^{\mathrm{mu}}_{\mathcal{C}}(\mathcal{A}) = u \cdot \mathbf{Adv}^{\mathrm{su}}_{\mathcal{C}}(\mathcal{A})$

PRF Security of XoP

- u: number of users
- q: total number of queries
- q_m: maximum number of queries per instance, $q_m \leq q \leq uq_m$
- P, Q: n-bit random permutations
- $\mathbf{Adv}_{\mathcal{C}}^{\mathrm{atk}}(q)$: the maximum of $\mathbf{Adv}_{\mathcal{C}}^{\mathrm{atk}}(\mathcal{A})$ among all $\mathcal{A}$ makes q queries

- The best known (multi-user) security bound for XoP2 from Mirror theory and the Squared-ratio method [CCL23, Crypto '23]:

$$\mathbf{Adv}_{\mathrm{XoP2}}^{\mathrm{prf}}(q) \leq O\left(\min\left\{\frac{q^2}{2^{2n}}, \frac{\sqrt{u}q_m^2}{2^{2n}}\right\}\right)$$

- Observation: XoP1 cannot output 0^n

$$\mathbf{Adv}_{\mathrm{XoP1}}^{\mathrm{prf}} = \frac{q}{2^n} \quad \text{(tight!)}$$

PRF Security of XoP

- u: number of users
- q: total number of queries
- q_m: maximum number of queries per instance, $q_m \le q \le uq_m$
- P, Q: n-bit random permutations
- $\mathbf{Adv}_{\mathcal{C}}^{\mathrm{atk}}(q)$: the maximum of $\mathbf{Adv}_{\mathcal{C}}^{\mathrm{atk}}(\mathcal{A})$ among all $\mathcal{A}$ makes q queries

- The best known (multi-user) security bound for XoP2 from Mirror theory and the Squared-ratio method [CCL23, Crypto '23]:

$$\mathbf{Adv}_{\mathrm{XoP2}}^{\mathrm{prf}}(q) \le O\left(\min\left\{\frac{q^2}{2^{2n}}, \frac{\sqrt{u}q_m^2}{2^{2n}}\right\}\right)$$

- Observation: XoP1 cannot output 0^n

$$\mathbf{Adv}_{\mathrm{XoP1}}^{\mathrm{prf}} = \frac{q}{2^n} \qquad \text{(tight!)}$$

PRF Security of XoP

- u: number of users
- q: total number of queries
- q_m: maximum number of queries per instance, $q_m \le q \le uq_m$
- P, Q: n-bit random permutations
- $\mathbf{Adv}_{\mathcal{C}}^{\mathrm{atk}}(q)$: the maximum of $\mathbf{Adv}_{\mathcal{C}}^{\mathrm{atk}}(\mathcal{A})$ among all $\mathcal{A}$ makes q queries

- The best known (multi-user) security bound for XoP2 from Mirror theory and the Squared-ratio method [CCL23, Crypto '23]:

$$\mathbf{Adv}_{\mathrm{XoP2}}^{\mathrm{prf}}(q) \le O\left(\min\left\{\frac{q^2}{2^{2n}}, \frac{\sqrt{u}q_m^2}{2^{2n}}\right\}\right)$$

- Observation: XoP1 cannot output 0^n

$$\mathbf{Adv}_{\mathrm{XoP1}}^{\mathrm{prf}} = \frac{q}{2^n} \quad \text{(tight!)}$$

MACs

- Generates tag to authenticate a given message
- Protects data integrity by verifying tag value
- XoP-based BBB secure MACs
  - Deterministic: DbHtS [DDNP18, ToSC '18]
  - Nonce-based: nEHtM [DNT19, EC '19]

MACs

- Generates tag to authenticate a given message
- Protects data integrity by verifying tag value
- XoP-based BBB secure MACs
  - Deterministic: DbHtS [DDNP18, ToSC '18]
  - Nonce-based: nEHtM [DNT19, EC '19]

MACs

- Generates tag to authenticate a given message
- Protects data integrity by verifying tag value
- XoP-based BBB secure MACs
    - Deterministic: DbHtS [DDNP18, ToSC '18]
    - Nonce-based: nEHtM [DNT19, EC '19]

DbHtS and nEHtM

- $\mathrm{H} = (\mathrm{H}^1, \mathrm{H}^2) : \{0,1\}^{2k} \times \mathcal{M} \to \{0,1\}^{n-1} \times \{0,1\}^{n-1}$:
  a $(2n-2)$-bit hash function where $\mathrm{H}_{K_h}(M) = (\mathrm{H}^1_{K_{h_1}}(M), \mathrm{H}^2_{K_{h_2}}(M))$
- $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$: a block cipher

- Define (modified) XoP1-based DbHtS and nEHtM:

$$\mathrm{DbHtS}[\mathrm{H}_{K_h}, \mathrm{E}_K](M) \stackrel{\text{def}}{=} \mathrm{E}_K(0 \| \mathrm{H}^1_{K_{h,1}}(M)) \oplus \mathrm{E}_K(1 \| \mathrm{H}^2_{K_{h,2}}(M))$$

$$\mathrm{nEHtM}[\mathrm{H}^1_{K_{h,1}}, \mathrm{E}_K](N, M) \stackrel{\text{def}}{=} \mathrm{E}_K(0 \| N) \oplus \mathrm{E}_K(1 \| \mathrm{H}^1_{K_{h,1}}(M) \oplus N)$$

DbHtS and nEHtM

- $\mathsf{H} = (\mathsf{H}^1, \mathsf{H}^2) : \{0,1\}^{2k} \times \mathcal{M} \to \{0,1\}^{n-1} \times \{0,1\}^{n-1}$: a $(2n-2)$-bit hash function where $\mathsf{H}_{K_h}(M) = (\mathsf{H}^1_{K_{h_1}}(M), \mathsf{H}^2_{K_{h_2}}(M))$
- $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$: a block cipher

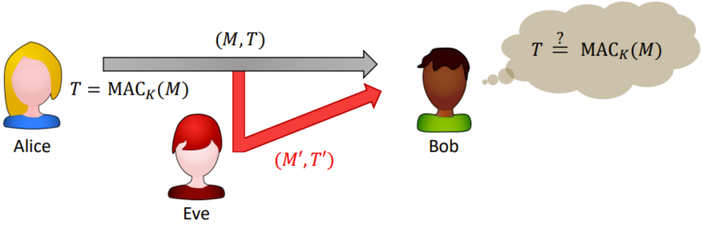
- Define (modified) XoP1-based DbHtS and nEHtM:

$$\mathsf{DbHtS}[\mathsf{H}_{K_h}, \mathsf{E}_K](M) \stackrel{\text{def}}{=} \mathsf{E}_K(0 \| \mathsf{H}^1_{K_{h,1}}(M)) \oplus \mathsf{E}_K(1 \| \mathsf{H}^2_{K_{h,2}}(M))$$

$$\mathsf{nEHtM}[\mathsf{H}^1_{K_{h,1}}, \mathsf{E}_K](N, M) \stackrel{\text{def}}{=} \mathsf{E}_K(0 \| N) \oplus \mathsf{E}_K(1 \| \mathsf{H}^1_{K_{h,1}}(M) \oplus N)$$

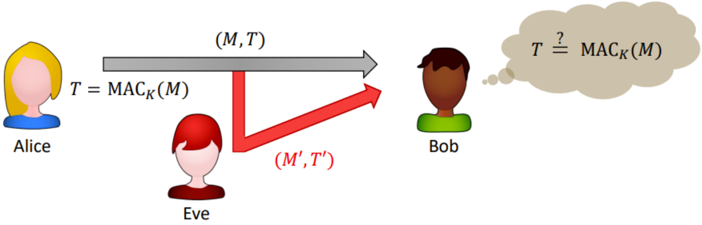
MAC Security: Deterministic Cases

- Unforgeability
  - Infeasible to generate a new valid message/tag pair
  - Allow q authentication queries and v verification queries to an adversary
- PRF security
  - Infeasible to distinguish from a random variable-input-length (VIL) function up to $(q+v)$ queries
  - $\Rightarrow$ a secure MAC, i.e., unforgeable



MAC Security: Deterministic Cases

- Unforgeability
  - Infeasible to generate a new valid message/tag pair
  - Allow q authentication queries and v verification queries to an adversary
- PRF security
  - Infeasible to distinguish from a random variable-input-length (VIL) function up to $(q + v)$ queries
  - $\Rightarrow$ a secure MAC, i.e., unforgeable



MAC Security: General Cases

- Unforgeability
  - Infeasible to generate a new valid message/tag pair
  - Allow q authentication queries and v verification queries
- PRF+@ security
  - Verification queries can do nonce-misuse
  - Infeasible to distinguish from a random VIL function for q authentication queries
  - Infeasible to distinguish from a "$\perp$ oracle" for v verification queries
  - $\Rightarrow$ a secure MAC

MAC Security: General Cases

- Unforgeability
  - Infeasible to generate a new valid message/tag pair
  - Allow q authentication queries and v verification queries

- PRF+@ security
  - Verification queries can do nonce-misuse
  - Infeasible to distinguish from a random VIL function for q authentication queries
  - Infeasible to distinguish from a "$\perp$ oracle" for v verification queries
  - $\Rightarrow$ a secure MAC

MAC Security

- Both cases need to show PRF security for q authentication queries

- But they are XoP1-based! So the adversarial advantage always exceeds $q/2^n$

Do Independent Two Permutations Yield Better Security Bound?

- $q/2^n$ is n-bit security, i.e., fully secure in some sense
- However, this is not always true in the multi-user setting
- [CCL23, Crypto '23] shows XoP2-based nEHtM may have a better (PRF) security bound than XoP1-based nEHtM for $q = uq_m$ case
  - Because $uq_m/2^n$ bound is inevitable for XoP1!

Do Independent Two Permutations Yield Better Security Bound?

- $q/2^n$ is n-bit security, i.e., fully secure in some sense
- However, this is not always true in the multi-user setting
- [CCL23, Crypto '23] shows XoP2-based nEHtM may have a better (PRF) security bound than XoP1-based nEHtM for $q = uq_m$ case
  - Because $uq_m/2^n$ bound is inevitable for XoP1!

Do Independent Two Permutations Yield Better Security Bound?

- $q/2^n$ is n-bit security, i.e., fully secure in some sense
- However, this is not always true in the multi-user setting
- [CCL23, Crypto '23] shows XoP2-based nEHtM may have a better (PRF) security bound than XoP1-based nEHtM for $q = uq_m$ case
  - Because $uq_m/2^n$ bound is inevitable for XoP1!

XoP1 Does Not Output 0^n

- But... wait, why do we need PRF security?
- While XoP1 does not output 0^n, why we need to assume the ideal world outputs 0^n?

- PRF security (for auth queries) is a sufficient condition but not a necessary conditoin to be a secure MAC
- Our ultimate goal is proving unforgeability

- We can freely choose the ideal world whatever we want, preferably uniformly random
- The ideal world should necessarily have enough entropy, i.e., a large range, but the range does not need to be $\{0,1\}^n$, e.g., it can be $\{0,1\}^n \setminus \{0^n\}$

XoP1 Does Not Output 0^n

- But... wait, why do we need PRF security?
- While XoP1 does not output 0^n, why we need to assume the ideal world outputs 0^n?

- PRF security (for auth queries) is a sufficient condition but not a necessary conditoin to be a secure MAC
- Our ultimate goal is proving unforgeability

- We can freely choose the ideal world whatever we want, preferably uniformly random
- The ideal world should necessarily have enough entropy, i.e., a large range, but the range does not need to be $\{0, 1\}^n$, e.g., it can be $\{0, 1\}^n \setminus \{0^n\}$

XoP1 Does Not Output 0^n

- But... wait, why do we need PRF security?
- While XoP1 does not output 0^n, why we need to assume the ideal world outputs 0^n?

- PRF security (for auth queries) is a sufficient condition but not a necessary conditoin to be a secure MAC
- Our ultimate goal is proving unforgeability

- We can freely choose the ideal world whatever we want, preferably uniformly random
- The ideal world should necessarily have enough entropy, i.e., a large range, but the range does not need to be $\{0, 1\}^n$, e.g., it can be $\{0, 1\}^n \setminus \{0^n\}$

How random XoP1 is?

- As a PRF maps to $\{0,1\}^n$: $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP1}} = \frac{q}{2^n}$
- How about as a PRF maps to $\{0,1\}^n \setminus \{0^n\}$?
- We define (multi-user) PRF* security by defining the ideal world as random samplings from $\{0,1\}^n \setminus \{0^n\}$ instead of $\{0,1\}^n$
  - Actually, by definition, this is also (mu) PRF security for the given range
  - We denote (mu) PRF security for indistinguishability from random functions maps $\{0,1\}^n$ to $\{0,1\}^n$

How random XoP1 is?

- As a PRF maps to $\{0,1\}^n$: $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP1}} = \frac{q}{2^n}$
- How about as a PRF maps to $\{0,1\}^n \setminus \{0^n\}$?
- We define (multi-user) PRF* security by defining the ideal world as random samplings from $\{0,1\}^n \setminus \{0^n\}$ instead of $\{0,1\}^n$
  - Actually, by definition, this is also (mu) PRF security for the given range
  - We denote (mu) PRF security for indistinguishability from random functions maps $\{0,1\}^n$ to $\{0,1\}^n$

How random XoP1 is?

- As a PRF maps to $\{0,1\}^n$: $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP1}} = \frac{q}{2^n}$
- How about as a PRF maps to $\{0,1\}^n \setminus \{0^n\}$?
- We define (multi-user) PRF* security by defining the ideal world as random samplings from $\{0,1\}^n \setminus \{0^n\}$ instead of $\{0,1\}^n$
  - Actually, by definition, this is also (mu) PRF security for the given range
  - We denote (mu) PRF security for indistinguishability from random functions maps $\{0,1\}^n$ to $\{0,1\}^n$

PRF* security of XoP1 — via the Chi-Squared Method

- We've found that PRF* security of XoP1 was already implicitly studied at [DHT17, Crypto '17],
  - proposed the Chi-squared method
  - proved PRF security of XoP1

- In their security proof, they implicitly proved (single-user) PRF* security of XoP1 as an intermediate step

- We prove (mu) prf* security of XoP1 using the Chi-squared method (NEW)

$$\mathbf{Adv}^{\mathrm{prf*}}_{\mathrm{XoP1}} \leq O\left(\frac{u^{0.5} {q_m}^{1.5}}{2^{1.5n}}\right)$$

This is almost the same as $\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{XoP2}}$ via the Chi-squared method

PRF* security of XoP1 — via the Chi-Squared Method

- We've found that PRF* security of XoP1 was already implicitly studied at [DHT17, Crypto '17],
  - proposed the Chi-squared method
  - proved PRF security of XoP1
- In their security proof, they implicitly proved (single-user) PRF* security of XoP1 as an intermediate step
- We prove (mu) prf* security of XoP1 using the Chi-squared method (NEW)

$$\mathbf{Adv}^{\mathrm{prf}*}_{\mathrm{XoP1}} \leq O\left(\frac{u^{0.5} {q_m}^{1.5}}{2^{1.5n}}\right)$$

This is almost the same as $\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{XoP2}}$ via the Chi-squared method

PRF* security of XoP1 — via the Chi-Squared Method

- We've found that PRF* security of XoP1 was already implicitly studied at [DHT17, Crypto '17],
  - proposed the Chi-squared method
  - proved PRF security of XoP1
- In their security proof, they implicitly proved (single-user) PRF* security of XoP1 as an intermediate step
- We prove (mu) prf* security of XoP1 using the Chi-squared method (NEW)

$$\mathbf{Adv}^{\mathrm{prf}*}_{\mathsf{XoP1}} \leq O\left(\frac{u^{0.5}{q_m}^{1.5}}{2^{1.5n}}\right)$$

This is almost the same as $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XoP2}}$ via the Chi-squared method

PRF* security of XoP1 — via the Squared-Ratio Method

- The Chi-squared method often leads to suboptimal results
  - e.g., one can obtain a better security bound of XoP2 from Mirror theory

- We prove (mu) PRF* security of XoP1 using the Squared-ratio method (NEW)

$$\mathbf{Adv}^{\mathrm{prf}*}_{\mathrm{XoP1}} \leq O\left(\frac{u^{0.5}{q_m}^2}{2^{2n}}\right)$$

- To prove this, we need to develop a NEW mirror theory
  1. in the fine-tuned setting
  2. for n-bit security
  3. both lower bound and upper bound

PRF* security of XoP1 — via the Squared-Ratio Method

- The Chi-squared method often leads to suboptimal results
  - e.g., one can obtain a better security bound of XoP2 from Mirror theory

- We prove (mu) PRF* security of XoP1 using the Squared-ratio method (NEW)

$$\mathbf{Adv}^{\mathrm{prf}*}_{\mathrm{XoP1}} \leq O\left(\frac{u^{0.5}{q_m}^2}{2^{2n}}\right)$$

- To prove this, we need to develop a NEW mirror theory
  1. in the fine-tuned setting
  2. for n-bit security
  3. both lower bound and upper bound

PRF* security of XoP1 — via the Squared-Ratio Method

- The Chi-squared method often leads to suboptimal results
  - e.g., one can obtain a better security bound of XoP2 from Mirror theory
- We prove (mu) PRF* security of XoP1 using the Squared-ratio method (NEW)

$$\mathbf{Adv}^{\mathrm{prf}*}_{\mathrm{XoP1}} \leq O\left(\frac{u^{0.5}{q_m}^2}{2^{2n}}\right)$$

- To prove this, we need to develop a NEW mirror theory
  1. in the fine-tuned setting
  2. for n-bit security
  3. both lower bound and upper bound

Security Comparison

- Via the Chi-squared method:

$$\mathbf{Adv}^{\mathrm{prf}*}_{\mathrm{XoP1}} \le O\left(\frac{u^{0.5}{q_m}^{1.5}}{2^{1.5n}}\right)$$

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{XoP2}} \le O\left(\frac{u^{0.5}{q_m}^{1.5}}{2^{1.5n}}\right)$$ [CKLL22, AC '22]

- Via the Squared-ratio method:

$$\mathbf{Adv}^{\mathrm{prf}*}_{\mathrm{XoP1}} \le O\left(\frac{u^{0.5}{q_m}^{2}}{2^{2n}}\right)$$

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{XoP2}} \le O\left(\frac{u^{0.5}{q_m}^{2}}{2^{2n}}\right)$$ [CCL23, Crypto '23]

- We conjecture XoP1 and XoP2 enjoy the (almost) same security bound by fine-tuning!

Security Comparison

- Via the Chi-squared method:

$$\mathbf{Adv}^{\mathrm{prf}*}_{\mathrm{XoP1}} \leq O\left(\frac{u^{0.5}{q_m}^{1.5}}{2^{1.5n}}\right)$$

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{XoP2}} \leq O\left(\frac{u^{0.5}{q_m}^{1.5}}{2^{1.5n}}\right)$$ [CKLL22, AC '22]

- Via the Squared-ratio method:

$$\mathbf{Adv}^{\mathrm{prf}*}_{\mathrm{XoP1}} \leq O\left(\frac{u^{0.5}{q_m}^{2}}{2^{2n}}\right)$$

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{XoP2}} \leq O\left(\frac{u^{0.5}{q_m}^{2}}{2^{2n}}\right)$$ [CCL23, Crypto '23]

- We conjecture XoP1 and XoP2 enjoy the (almost) same security bound by fine-tuning!

Security Comparison

- Via the Chi-squared method:

$$\mathbf{Adv}^{\mathrm{prf}*}_{\mathrm{XoP1}} \leq O\left(\frac{u^{0.5}{q_m}^{1.5}}{2^{1.5n}}\right)$$

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{XoP2}} \leq O\left(\frac{u^{0.5}{q_m}^{1.5}}{2^{1.5n}}\right)$$ [CKLL22, AC '22]

- Via the Squared-ratio method:

$$\mathbf{Adv}^{\mathrm{prf}*}_{\mathrm{XoP1}} \leq O\left(\frac{u^{0.5}{q_m}^{2}}{2^{2n}}\right)$$

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{XoP2}} \leq O\left(\frac{u^{0.5}{q_m}^{2}}{2^{2n}}\right)$$ [CCL23, Crypto '23]

- We conjecture XoP1 and XoP2 enjoy the (almost) same security bound by fine-tuning!

Fine-Tuning Mirror Theory

- Mirror theory can give a sharp lower bound of the number of solutions, $h(\Gamma)$, to the given system Γ (and let $N = 2^n$):

$$h(\Gamma) \geq \frac{(N)_{q_P}}{N^q}$$

- In the "fine-tuned" ideal world, we want to have $\epsilon \ll \frac{q}{N}$ s.t.

$$h(\Gamma) \geq (1-\epsilon) \times \frac{(N)_{q_P}}{(N-1)^q}$$

- However, it cannot be directly derived from the previous result

$$h(\Gamma) \geq \frac{(N-1)^q}{N^q} \times \frac{(N)_{q_P}}{(N-1)^q}$$
$$\geq \left(1 - \frac{q}{N}\right) \times \frac{(N)_{q_P}}{(N-1)^q}$$

Fine-Tuning Mirror Theory

- Mirror theory can give a sharp lower bound of the number of solutions, $h(\Gamma)$, to the given system Γ (and let $N = 2^n$):

$$h(\Gamma) \geq \frac{(N)_{q_P}}{N^q}$$

- In the "fine-tuned" ideal world, we want to have $\epsilon \ll \frac{q}{N}$ s.t.

$$h(\Gamma) \geq (1-\epsilon) \times \frac{(N)_{q_P}}{(N-1)^q}$$

- However, it cannot be directly derived from the previous result

$$h(\Gamma) \geq \frac{(N-1)^q}{N^q} \times \frac{(N)_{q_P}}{(N-1)^q}$$
$$\geq \left(1 - \frac{q}{N}\right) \times \frac{(N)_{q_P}}{(N-1)^q}$$

Fine-Tuning Mirror Theory

- Mirror theory can give a sharp lower bound of the number of solutions, $h(\Gamma)$, to the given system Γ (and let $N = 2^n$):

$$h(\Gamma) \geq \frac{(N)_{q_P}}{N^q}$$

- In the "fine-tuned" ideal world, we want to have $\epsilon \ll \frac{q}{N}$ s.t.

$$h(\Gamma) \geq (1 - \epsilon) \times \frac{(N)_{q_P}}{(N-1)^q}$$

- However, it cannot be directly derived from the previous result

$$h(\Gamma) \geq \frac{(N-1)^q}{N^q} \times \frac{(N)_{q_P}}{(N-1)^q}$$
$$\geq \left(1 - \frac{q}{N}\right) \times \frac{(N)_{q_P}}{(N-1)^q}$$

Variants of Mirror Theory

- From direct derivation, we have the $\frac{q}{N}$ term, which is what we want to avoid

- It implies that the previous Mirror theory loosely bounds $h(\Gamma)$!

- Hence, we need to develop a new Mirror theory such that
  1. Fine-tuned — more tightly
  2. for n-bit security for $\xi_{\max} = 2$
  3. for $3n/4$-bit security for any $\xi_{\max}$
  4. extended to handle verification queries (non-equations)
  5. both lower bound and upper bound to apply the Squared-ratio method

Variants of Mirror Theory

- From direct derivation, we have the $\frac{q}{N}$ term, which is what we want to avoid
- It implies that the previous Mirror theory loosely bounds $h(\Gamma)$!
- Hence, we need to develop a new Mirror theory such that
  1. Fine-tuned — more tightly
  2. for n-bit security for $\xi_{\max} = 2$
  3. for $3n/4$-bit security for any $\xi_{\max}$
  4. extended to handle verification queries (non-equations)
  5. both lower bound and upper bound to apply the Squared-ratio method

Variants of Mirror Theory

- From direct derivation, we have the $\frac{q}{N}$ term, which is what we want to avoid
- It implies that the previous Mirror theory loosely bounds $h(\Gamma)$!
- Hence, we need to develop a new Mirror theory such that
  1. Fine-tuned — more tightly
  2. for n-bit security for $\xi_{\max} = 2$
  3. for $3n/4$-bit security for any $\xi_{\max}$
  4. extended to handle verification queries (non-equations)
  5. both lower bound and upper bound to apply the Squared-ratio method

Variants of Mirror Theory

- From direct derivation, we have the $\frac{q}{N}$ term, which is what we want to avoid
- It implies that the previous Mirror theory loosely bounds $h(\Gamma)$!
- Hence, we need to develop a new Mirror theory such that
  1. Fine-tuned — more tightly
  2. for n-bit security for $\xi_{\max} = 2$
  3. for $3n/4$-bit security for any $\xi_{\max}$
  4. extended to handle verification queries (non-equations)
  5. both lower bound and upper bound to apply the Squared-ratio method

Variants of Mirror Theory

- From direct derivation, we have the $\frac{q}{N}$ term, which is what we want to avoid

- It implies that the previous Mirror theory loosely bounds $h(\Gamma)$!

- Hence, we need to develop a new Mirror theory such that
  1. Fine-tuned — more tightly
  2. for n-bit security for $\xi_{\max} = 2$
  3. for $3n/4$-bit security for any $\xi_{\max}$
  4. extended to handle verification queries (non-equations)
  5. both lower bound and upper bound to apply the Squared-ratio method

Variants of Mirror Theory

- From direct derivation, we have the $\frac{q}{N}$ term, which is what we want to avoid
- It implies that the previous Mirror theory loosely bounds $h(\Gamma)$!
- Hence, we need to develop a new Mirror theory such that
  1. Fine-tuned — more tightly
  2. for n-bit security for $\xi_{\max} = 2$
  3. for $3n/4$-bit security for any $\xi_{\max}$
  4. extended to handle verification queries (non-equations)
  5. both lower bound and upper bound to apply the Squared-ratio method

Variants of Mirror Theory

- From direct derivation, we have the $\frac{q}{N}$ term, which is what we want to avoid
- It implies that the previous Mirror theory loosely bounds $h(\Gamma)$!
- Hence, we need to develop a new Mirror theory such that
  1. Fine-tuned — more tightly
  2. for n-bit security for $\xi_{\max} = 2$
  3. for $3n/4$-bit security for any $\xi_{\max}$
  4. extended to handle verification queries (non-equations)
  5. both lower bound and upper bound to apply the Squared-ratio method

Variants of Mirror Theory

- From direct derivation, we have the $\frac{q}{N}$ term, which is what we want to avoid
- It implies that the previous Mirror theory loosely bounds $h(\Gamma)$!
- Hence, we need to develop a new Mirror theory such that
  1. Fine-tuned — more tightly
  2. for n-bit security for $\xi_{\max} = 2$
  3. for $3n/4$-bit security for any $\xi_{\max}$
  4. extended to handle verification queries (non-equations)
  5. both lower bound and upper bound to apply the Squared-ratio method

Proving MAC Security through PRF*

- PRF* security suffices for MAC security
  - authentication queries $\approx$ random function queries not outputting 0^n
  - verification queries $\approx$ "$\perp$ oracle" queries
  - $\Rightarrow$ a secure MAC
- (Multi-user) MAC security using the fine-tuned ideal world!
  - removing the $q/2^n$ barrier for the single permutation primitives
  - using fine-tuned mirror theory and bad events (as in PRF*)
  - obtaining better mu security for nEHtM and DbHtS

Proving MAC Security through PRF*

- PRF* security suffices for MAC security
  - authentication queries $\approx$ random function queries not outputting 0^n
  - verification queries $\approx$ "$\perp$ oracle" queries
  - $\Rightarrow$ a secure MAC
- (Multi-user) MAC security using the fine-tuned ideal world!
  - removing the $q/2^n$ barrier for the single permutation primitives
  - using fine-tuned mirror theory and bad events (as in PRF*)
  - obtaining better mu security for nEHtM and DbHtS

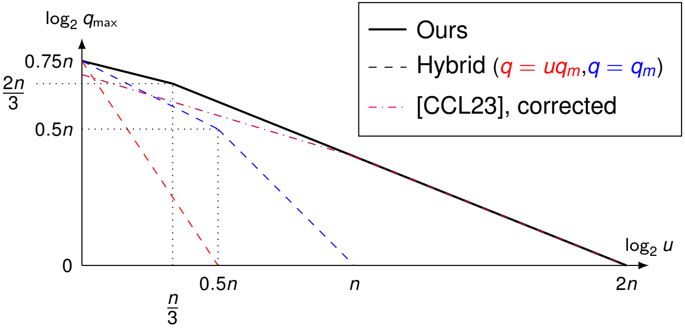
Improved mu-MAC Security of nEHtM

- Security of nEHtM, in terms of the thresholds

	#Query q_m	#User u	#Perm	Security
[DNT19]	$2^{0.66n}$	-	1	su-MAC
[CLLL20]	$2^{0.75n}$	-	1	su-MAC
[CCL23]	$2^{0.7n}$	2^{2n} (*)	2	mu-PRF
This work	$2^{0.75n}$	2^{2n}	1	mu-MAC

  - The query threshold q_m is per user (u is small for mu security)
  - The user threshold u is for small q_m
  - The bug (*) in [CCL23] is corrected in our paper

Graphical Comparison



Previous Multi-User PRF Security of DbHtS

- [SWGW21, Crypto '21] proved $2/3n$-bit security
- Their DbHtS construction assumes the underlying hash function is regular, AU, and based on ideal cipher

- [DDNT23, ToSC '23] proved $3/4n$-bit security
- Their DbHtS construction assumes the underlying hash function is regular, AU, and cross-collision resistant

Previous Multi-User PRF Security of DbHtS

- [SWGW21, Crypto '21] proved $2/3n$-bit security
- Their DbHtS construction assumes the underlying hash function is regular, AU, and based on ideal cipher

- [DDNT23, ToSC '23] proved $3/4n$-bit security
- Their DbHtS construction assumes the underlying hash function is regular, AU, and cross-collision resistant

Multi-User PRF* Security of DbHtS

- We prove mu-PRF* security of DbHtS in both settings: [SWGW21, Crypto '21] and [DDNT23, ToSC '23]
- ...but introducing q_m to achieve better bounds!
- We assume a stronger hash property to improve [DDNT23]

Multi-User PRF* Security of DbHtS

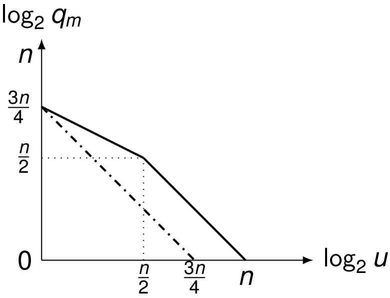
- We prove mu-PRF* security of DbHtS in both settings: [SWGW21, Crypto '21] and [DDNT23, ToSC '23]
- ...but introducing q_m to achieve better bounds!
- We assume a stronger hash property to improve [DDNT23]

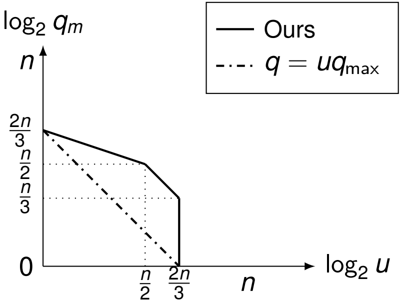
Multi-User PRF* Security of DbHtS

- We prove mu-PRF* security of DbHtS in both settings: [SWGW21, Crypto '21] and [DDNT23, ToSC '23]
- ...but introducing q_m to achieve better bounds!
- We assume a stronger hash property to improve [DDNT23]

Security Comparison

- The right figure compares our result with [DDNT23] and the left one compares ours with [SWGW21]





Conclusion

New results

- Deeper understanding about fundamental XoP1
- New tighter fine-tuned extended mirror theory with an upper bound for n-bit or any $\xi_{\max}$
- Improved multi-user security of nEHtM and DbHtS
- Fixing a flaw in the previous multi-user result of nEHtM

Future research

- Fine-tuning other security notions (Encryption?)
- Improving better security bounds (without assuming a stronger hash for DbHtS)

Thank you for your attention!

Conclusion

New results

- Deeper understanding about fundamental XoP1
- New tighter fine-tuned extended mirror theory with an upper bound for n-bit or any $\xi_{\max}$
- Improved multi-user security of nEHtM and DbHtS
- Fixing a flaw in the previous multi-user result of nEHtM

Future research

- Fine-tuning other security notions (Encryption?)
- Improving better security bounds (without assuming a stronger hash for DbHtS)

Thank you for your attention!

Conclusion

New results

- Deeper understanding about fundamental XoP1
- New tighter fine-tuned extended mirror theory with an upper bound for n-bit or any $\xi_{\max}$
- Improved multi-user security of nEHtM and DbHtS
- Fixing a flaw in the previous multi-user result of nEHtM

Future research

- Fine-tuning other security notions (Encryption?)
- Improving better security bounds (without assuming a stronger hash for DbHtS)

Thank you for your attention!

Chi-Squared Method [DHT17]

- $Z^i_{\mathcal{S}}$: a random variable over Ω that follows
  - the distribution of the i-th answer obtained by $\mathcal{A}$ interacting with $\mathcal{S}$

$$\mathsf{p}^{\mathbf{z}}_{\mathcal{S}}(z) \stackrel{\text{def}}{=} \Pr\left[Z^i_{\mathcal{S}} = z \mid (Z^1_{\mathcal{S}}, \ldots, Z^{i-1}_{\mathcal{S}}) = \mathbf{z}\right]$$

- Chi-squared method:

$$\|\mathsf{p}_{\mathcal{S}_0}(\cdot) - \mathsf{p}_{\mathcal{S}_1}(\cdot)\| \leq \left(\frac{1}{2}\sum_{i=1}^{q} \mathop{\mathbf{Ex}}_{\mathbf{z}}\left[\chi^2(\mathbf{z})\right]\right)^{\frac{1}{2}}$$

where the expectation is taken over the real world and

$$\chi^2(\mathbf{z}) \stackrel{\text{def}}{=} \sum_{z \in \Omega} \frac{\left(\mathsf{p}^{\mathbf{z}}_{\mathcal{S}_1}(z) - \mathsf{p}^{\mathbf{z}}_{\mathcal{S}_0}(z)\right)^2}{\mathsf{p}^{\mathbf{z}}_{\mathcal{S}_0}(z)}$$

Patarin's H-coefficient Technique

- For any good transcript z, it holds

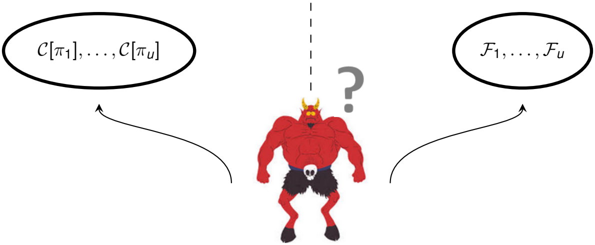
$$\frac{P_{S_1}(z)}{P_{S_0}(z)} \geq 1 - \epsilon$$

- Then we have

$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + \Pr[Z_{\mathcal{S}_0} \in \mathcal{T}_{\text{bad}}]$$

- $\mathcal{T}_{\text{bad}}$ and ϵ: depend on the construction
- $\Pr[Z_{\mathcal{S}_0} \in \mathcal{T}_{\text{bad}}]$: a combinatorial problem relies on the randomness in the ideal world

Squared-Ratio Method: The Idea

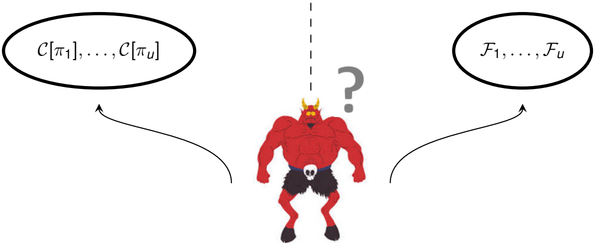


attacker $\mathcal{A}$

- $\mathcal{A}$ is allowed to make q_m queries to each user $i \in [u]$
- Transcripts from the other users cannot contribute an information-theoretic adversary's query choice
  $\rightarrow$ the systems are mutually independent:

$$\mathrm{p}_{\mathcal{S}_i}(\mathbf{z}) = \prod_{j=1}^{u} \mathrm{p}_{\mathcal{S}_{i,j}}(z_j)$$

Squared-Ratio Method: The Idea



attacker $\mathcal{A}$

- $\mathcal{A}$ is allowed to make q_m queries to each user $i \in [u]$
- Transcripts from the other users cannot contribute an information-theoretic adversary's query choice
  $\rightarrow$ the systems are mutually independent:

$$\mathrm{p}_{\mathcal{S}_i}(\mathbf{z}) = \prod_{j=1}^{u} \mathrm{p}_{\mathcal{S}_{i,j}}(z_j)$$

Squared-Ratio Method [CCL23]

- For any good transcript z, it holds

$$\left| \frac{P_{S_1,1}(z)}{P_{S_0,1}(z)} - 1 \right| \leq \epsilon(z)$$

- Then we have

$$\|\mathrm{p}_{\mathcal{S}_1}(\cdot) - \mathrm{p}_{\mathcal{S}_0}(\cdot)\| \leq \sqrt{2u \cdot \mathbf{Ex}\left[\epsilon(z)^2\right]} + 2u \cdot \Pr[Z_{\mathcal{S}_0} \in \mathcal{T}_{\mathrm{bad}}]$$

where the expectation is taken over the ideal world

Squared-Ratio Method [CCL23]

- For any good transcript z, it holds

$$\left| \frac{P_{S_1,1}(z)}{P_{S_0,1}(z)} - 1 \right| \leq \epsilon(z)$$

- Then we have

$$\|\mathrm{p}_{\mathcal{S}_1}(\cdot) - \mathrm{p}_{\mathcal{S}_0}(\cdot)\| \leq \sqrt{2u \cdot \mathbf{Ex}\left[\epsilon(z)^2\right]} + 2u \cdot \Pr[Z_{\mathcal{S}_0} \in \mathcal{T}_{\mathrm{bad}}]$$

where the expectation is taken over the ideal world

System of Equations — from Single Permutation

- A set of unknowns $\mathcal{P} = \{P_1, \ldots, P_{q_P}\}$ and knowns values $\lambda_1, \ldots, \lambda_q$
- A system of equations

$$\Gamma : \begin{cases} P_{\varphi(1)} \oplus P_{\varphi'(1)} = \lambda_1, \\ P_{\varphi(2)} \oplus P_{\varphi'(2)} = \lambda_2, \\ \qquad \vdots \\ P_{\varphi(q)} \oplus P_{\varphi'(q)} = \lambda_q, \end{cases}$$

where φ and φ' are two surjective index mappings such that

$$\varphi \colon \{1, \ldots, q\} \to \{1, \ldots, q_P\},$$
$$\varphi' \colon \{1, \ldots, q\} \to \{1, \ldots, q_P\},$$

- Mirror theory gives a lower bound on the number of solutions of these systems

Patarin's Mirror Theory

- Represents the system of equations by a graph
  - A distinct unknown $\rightarrow$ a vertex with unknown value
  - An equation $\rightarrow$ a λ-labeled edge

- Transcript graph should be
  - acyclic
  - non-zero path label (non-degenerate)

- In the "fine-tuned" ideal world, we need an additional condition: $\lambda \neq 0^n$

Patarin's Mirror Theory

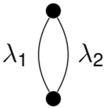
- Represents the system of equations by a graph
  - A distinct unknown $\rightarrow$ a vertex with unknown value
  - An equation $\rightarrow$ a λ-labeled edge

- Transcript graph should be
  - acyclic
  - non-zero path label (non-degenerate)

- In the "fine-tuned" ideal world, we need an additional condition: $\lambda \neq 0^n$

Patarin's Mirror Theory

- Represents the system of equations by a graph
  - A distinct unknown $\to$ a vertex with unknown value
  - An equation $\to$ a λ-labeled edge
- Transcript graph should be
  - acyclic
  - non-zero path label (non-degenerate)



- In the "fine-tuned" ideal world, we need an additional condition: $\lambda \neq 0^n$

Patarin's Mirror Theory

- Represents the system of equations by a graph
  - A distinct unknown $\rightarrow$ a vertex with unknown value
  - An equation $\rightarrow$ a λ-labeled edge

- Transcript graph should be
  - acyclic
  - non-zero path label (non-degenerate)

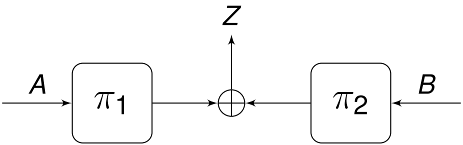
- In the "fine-tuned" ideal world, we need an additional condition: $\lambda \neq 0^n$

Patarin's Mirror Theory

- Represents the system of equations by a graph
  - A distinct unknown $\rightarrow$ a vertex with unknown value
  - An equation $\rightarrow$ a λ-labeled edge
- Transcript graph should be
  - acyclic
  - non-zero path label (non-degenerate)

- In the "fine-tuned" ideal world, we need an additional condition: $\lambda \neq 0^n$

Framework For Use

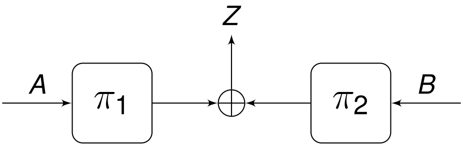


- Query transcript $\tau = \{(A_1, B_1, Z_1), \ldots, (A_q, B_q, Z_q)\}$
- Each such algorithm consists of an evaluation of π_1 and an evaluation of π_2

$$\Gamma = \begin{cases} \pi_1(A_1) \oplus \pi_2(B_1) = Z_1, \\ \vdots \\ \pi_1(A_q) \oplus \pi_2(B_q) = Z_q. \end{cases}$$

- Define $\mathcal{T}_{\text{bad}}$ such that the graph is consistent
- Obtain ϵ using mirror theory

Framework For Use

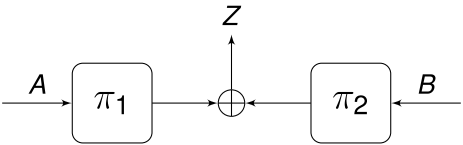


- Query transcript $\tau = \{(A_1, B_1, Z_1), \ldots, (A_q, B_q, Z_q)\}$
- Each such algorithm consists of an evaluation of π_1 and an evaluation of π_2

$$\Gamma = \begin{cases} \pi_1(A_1) \oplus \pi_2(B_1) = Z_1, \\ \vdots \\ \pi_1(A_q) \oplus \pi_2(B_q) = Z_q. \end{cases}$$

- Define $\mathcal{T}_{\text{bad}}$ such that the graph is consistent
- Obtain ϵ using mirror theory

Framework For Use

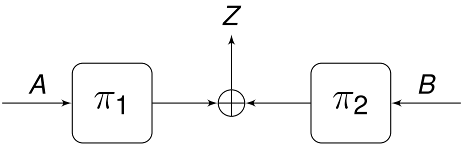


- Query transcript $\tau = \{(A_1, B_1, Z_1), \ldots, (A_q, B_q, Z_q)\}$
- Each such algorithm consists of an evaluation of π_1 and an evaluation of π_2

$$\Gamma = \begin{cases} \pi_1(A_1) \oplus \pi_2(B_1) = Z_1, \\ \vdots \\ \pi_1(A_q) \oplus \pi_2(B_q) = Z_q. \end{cases}$$

- Define $\mathcal{T}_{\text{bad}}$ such that the graph is consistent
- Obtain ϵ using mirror theory

Framework For Use

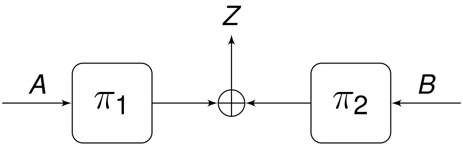


- Query transcript $\tau = \{(A_1, B_1, Z_1), \ldots, (A_q, B_q, Z_q)\}$
- Each such algorithm consists of an evaluation of π_1 and an evaluation of π_2

$$\Gamma = \begin{cases} \pi_1(A_1) \oplus \pi_2(B_1) = Z_1, \\ \vdots \\ \pi_1(A_q) \oplus \pi_2(B_q) = Z_q. \end{cases}$$

- Define $\mathcal{T}_{\text{bad}}$ such that the graph is consistent
- Obtain ϵ using mirror theory

Framework For Use



- Query transcript $\tau = \{(A_1, B_1, Z_1), \ldots, (A_q, B_q, Z_q)\}$
- Each such algorithm consists of an evaluation of π_1 and an evaluation of π_2

$$\Gamma = \begin{cases} \pi_1(A_1) \oplus \pi_2(B_1) = Z_1, \\ \vdots \\ \pi_1(A_q) \oplus \pi_2(B_q) = Z_q. \end{cases}$$

- Define $\mathcal{T}_{\text{bad}}$ such that the graph is consistent
- Obtain ϵ using mirror theory