Improved Multi-User Security Using the Squared-Ratio Method

Yu Long Chen[1] **Wonseok Choi**[2] Changmin Lee[3]

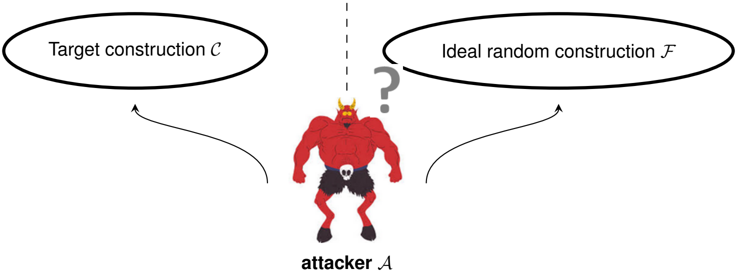
[1]imec-COSIC, KU Leuven, Belgium

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

[3]KIAS, Seoul, Korea

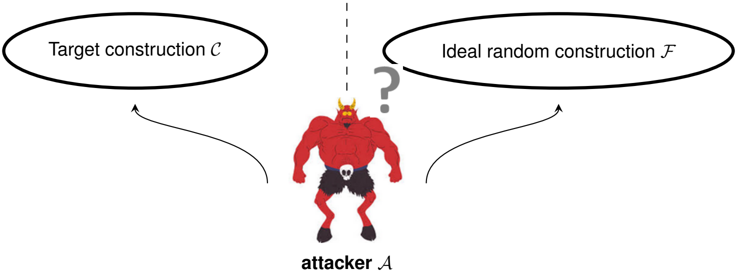
August 23th, 2023

Generic Single-User Security



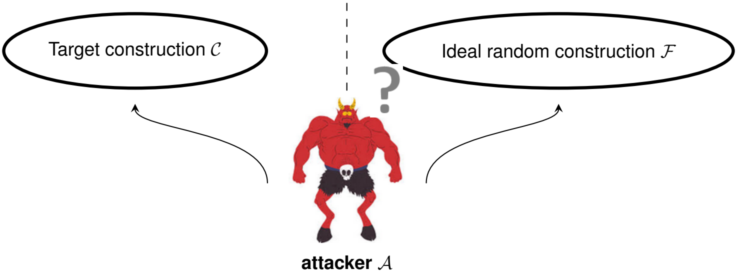
- $\mathcal{A}$ makes q queries to the construction oracle ($\mathcal{C}$ or $\mathcal{F}$)
- Security: a distinguishing probability of the two worlds:
  - $\mathbf{Adv}^{\mathsf{su}}_{\mathcal{C}}(\mathcal{A})$ can be denoted as a function of q
- $\mathbf{Adv}^{\mathsf{su}}_{\mathcal{C}}(\mathcal{A})$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

Generic Single-User Security



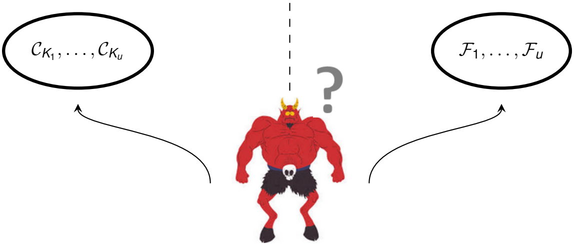
- $\mathcal{A}$ makes q queries to the construction oracle ($\mathcal{C}$ or $\mathcal{F}$)
- Security: a distinguishing probability of the two worlds:
  - $\mathbf{Adv}^{\mathrm{su}}_{\mathcal{C}}(\mathcal{A})$ can be denoted as a function of q
- $\mathbf{Adv}^{\mathrm{su}}_{\mathcal{C}}(\mathcal{A})$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

Generic Single-User 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

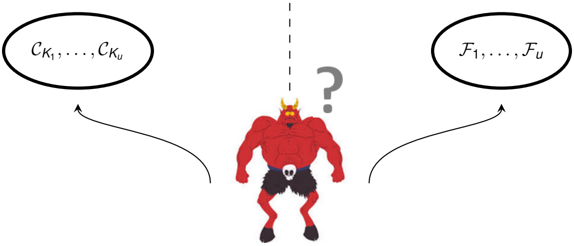
Generic Multi-User Security



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 $\mathbf{Adv}^{\mathrm{mu}}_{\mathcal{C}}(\mathcal{A}) = u \cdot \mathbf{Adv}^{\mathrm{su}}_{\mathcal{C}}(\mathcal{A})$

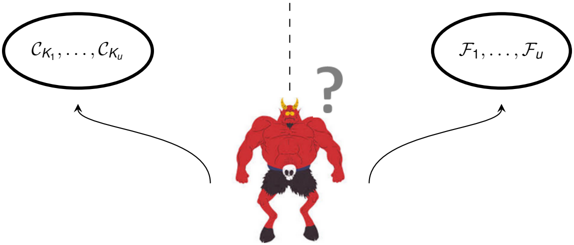
Generic Multi-User Security



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 $\mathbf{Adv}^{\mathrm{mu}}_{\mathcal{C}}(\mathcal{A}) = u \cdot \mathbf{Adv}^{\mathrm{su}}_{\mathcal{C}}(\mathcal{A})$

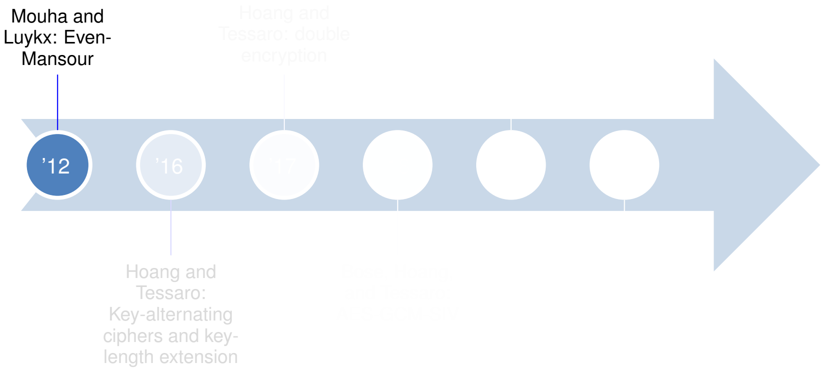
Generic Multi-User Security



attacker $\mathcal{A}$

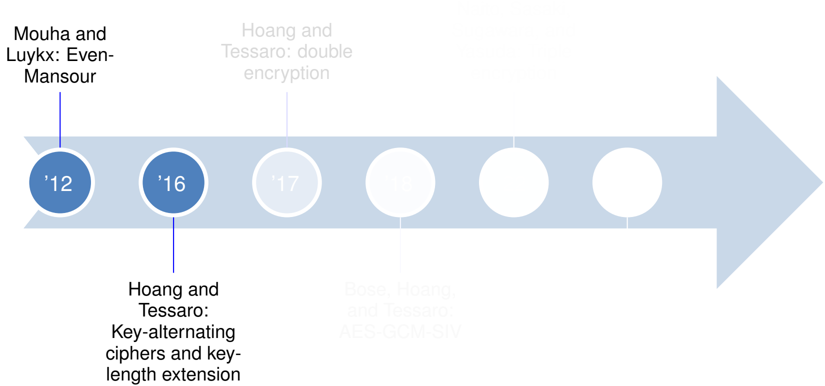
- $\mathcal{A}$ makes q queries to u construction oracles ($\mathcal{C}_{K_1}, \ldots, \mathcal{C}_{K_u}$ or $\mathcal{F}_1, \ldots, \mathcal{F}_u$)
- $\mathcal{A}$ succeeds as long as it can compromise K_i for any i
- Naive hybrid argument $\mathbf{Adv}^{\mathrm{mu}}_{\mathcal{C}}(\mathcal{A}) = u \cdot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

History of Symmetric-Key Multi-User Security: Some Examples



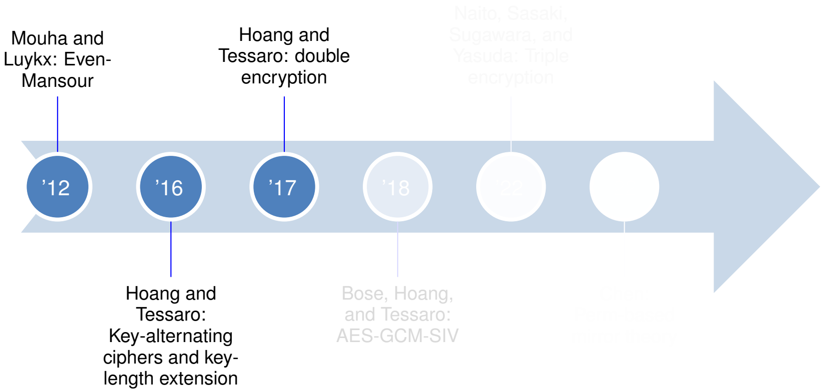
But there are more!

History of Symmetric-Key Multi-User Security: Some Examples



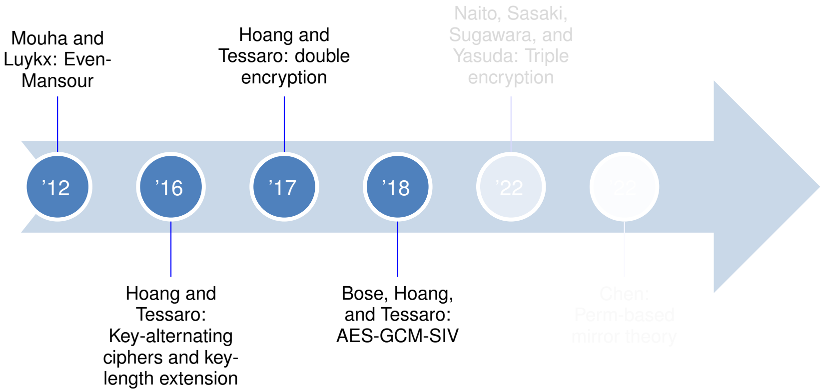
But there are more!

History of Symmetric-Key Multi-User Security: Some Examples



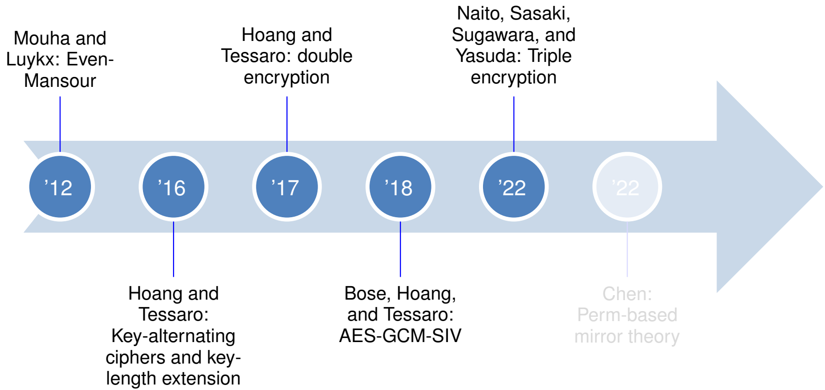
But there are more!

History of Symmetric-Key Multi-User Security: Some Examples



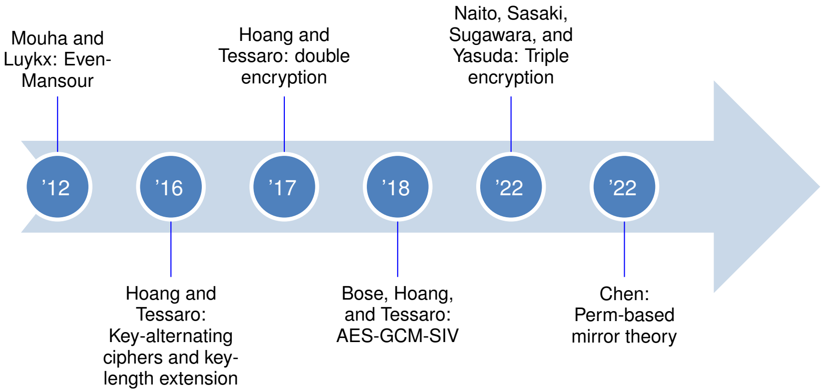
But there are more!

History of Symmetric-Key Multi-User Security: Some Examples



But there are more!

History of Symmetric-Key Multi-User Security: Some Examples



But there are more!

A Different Avenue

- Bhattacharya and Nandi (AC2021): XORP[3]
  - $\mathbf{Adv}^{\mathrm{mu}}_{\mathrm{XORP[3]}}(\mathcal{A}) < \frac{\sqrt{u \cdot q_{\max}}}{2^n}$
  - u = number of users, $q_{\max}$ = allowed number of queries to each user
  - In the standard model via the Chi-squared method
- CKLL (AC2022): SaT1, SaT2, and a variant of XORP[3]
  - Observe that it might be possible: $\mathbf{Adv}^{\mathrm{mu}}_{\mathcal{C}}(\mathcal{A}) = \sqrt{u} \cdot \mathbf{Adv}^{\mathrm{su}}_{\mathcal{C}}(\mathcal{A})$

However . . .

- Limitations of the Chi-squared method
  - Not easily generalized, especially hash-based constructions
  - Hard to achieve a tight bound

A Different Avenue

- Bhattacharya and Nandi (AC2021): XORP[3]
  - $\mathbf{Adv}^{\mathrm{mu}}_{\mathrm{XORP[3]}}(\mathcal{A}) < \frac{\sqrt{u \cdot q_{\max}}}{2^n}$
  - u = number of users, $q_{\max}$ = allowed number of queries to each user
  - In the standard model via the Chi-squared method
- CKLL (AC2022): SaT1, SaT2, and a variant of XORP[3]
  - Observe that it might be possible: $\mathbf{Adv}^{\mathrm{mu}}_{\mathcal{C}}(\mathcal{A}) = \sqrt{u} \cdot \mathbf{Adv}^{\mathrm{su}}_{\mathcal{C}}(\mathcal{A})$

However . . .

- Limitations of the Chi-squared method
  - Not easily generalized, especially hash-based constructions
  - Hard to achieve a tight bound

A Different Avenue

- Bhattacharya and Nandi (AC2021): XORP[3]
  - $\mathbf{Adv}^{\text{mu}}_{\text{XORP[3]}}(\mathcal{A}) < \frac{\sqrt{u \cdot q_{\max}}}{2^n}$
  - u = number of users, $q_{\max}$ = allowed number of queries to each user
  - In the standard model via the Chi-squared method
- CKLL (AC2022): SaT1, SaT2, and a variant of XORP[3]
  - Observe that it might be possible: $\mathbf{Adv}^{\text{mu}}_{\mathcal{C}}(\mathcal{A}) = \sqrt{u} \cdot \mathbf{Adv}^{\text{su}}_{\mathcal{C}}(\mathcal{A})$

However . . .

- Limitations of the Chi-squared method
  - Not easily generalized, especially hash-based constructions
  - Hard to achieve a tight bound

A Different Avenue

- Bhattacharya and Nandi (AC2021): XORP[3]
  - $\mathbf{Adv}^{\text{mu}}_{\text{XORP[3]}}(\mathcal{A}) < \frac{\sqrt{u \cdot q_{\text{max}}}}{2^n}$
  - u = number of users, q_{max} = allowed number of queries to each user
  - In the standard model via the Chi-squared method
- CKLL (AC2022): SaT1, SaT2, and a variant of XORP[3]
  - Observe that it might be possible: $\mathbf{Adv}^{\text{mu}}_{\mathcal{C}}(\mathcal{A}) = \sqrt{u} \cdot \mathbf{Adv}^{\text{su}}_{\mathcal{C}}(\mathcal{A})$

However . . .

- Limitations of the Chi-squared method
  - Not easily generalized, especially hash-based constructions
  - Hard to achieve a tight bound

Our Contribution - in a Nutshell

A NEW technique to prove multi-user security!

Three components:

- The Squared-Ratio method: a new framework for multi-user security proofs
- An upper bound for mirror theory
- Application to the multi-user security of XoP, EDM, and nEHtM

modular proofs from su *to* mu AND *improved multi-user bounds*

Our Contribution - in a Nutshell

A NEW technique to prove multi-user security!

Three components:

- The Squared-Ratio method: a new framework for multi-user security proofs
- An upper bound for mirror theory
- Application to the multi-user security of XoP, EDM, and nEHtM

modular proofs from su *to* mu AND *improved multi-user bounds*

Our Contribution - in a Nutshell

A NEW technique to prove multi-user security!

Three components:

- The Squared-Ratio method: a new framework for multi-user security proofs
- An upper bound for mirror theory
- Application to the multi-user security of XoP, EDM, and nEHtM

modular proofs from su *to* mu AND *improved multi-user bounds*

Our Contribution - in a Nutshell

A NEW technique to prove multi-user security!

Three components:

- The Squared-Ratio method: a new framework for multi-user security proofs
- An upper bound for mirror theory
- Application to the multi-user security of XoP, EDM, and nEHtM

modular proofs from su *to* mu AND *improved multi-user bounds*

Our Contribution - in a Nutshell

A NEW technique to prove multi-user security!

Three components:

- The Squared-Ratio method: a new framework for multi-user security proofs
- An upper bound for mirror theory
- Application to the multi-user security of XoP, EDM, and nEHtM

modular proofs from su *to* mu AND *improved multi-user bounds*

Our Contribution - in a Nutshell

A NEW technique to prove multi-user security!

Three components:

- The Squared-Ratio method: a new framework for multi-user security proofs
- An upper bound for mirror theory
- Application to the multi-user security of XoP, EDM, and nEHtM

modular proofs from su *to* mu AND *improved multi-user bounds*

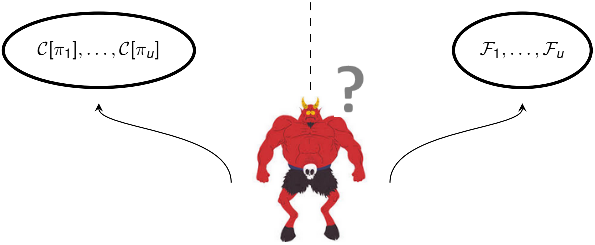
The Chi-Squared Method

- Introduced by Dai, Hoang, and Tessaro (CR '17)
- Bound the statistical distance of $\|\mathrm{p}_{\mathcal{S}_1}(\cdot) - \mathrm{p}_{\mathcal{S}_0}(\cdot)\|$
- The method utilizes well-known inequalities between the statistical distance, KL divergence, and Chi-squared divergence

$$\|\mathrm{p}_{\mathcal{S}_1}(\cdot) - \mathrm{p}_{\mathcal{S}_0}(\cdot)\| \leq \left(\frac{1}{2}\Delta_{KL}\left(\mathrm{p}_{\mathcal{S}_1}(\cdot), \mathrm{p}_{\mathcal{S}_0}(\cdot)\right)\right)^{\frac{1}{2}},$$

$$\Delta_{KL}\left(\mathrm{p}_{\mathcal{S}_1}(\cdot), \mathrm{p}_{\mathcal{S}_0}(\cdot)\right) \leq \sum_{z\in\Omega} \frac{\left(\mathrm{p}_{\mathcal{S}_1}(z) - \mathrm{p}_{\mathcal{S}_0}(z)\right)^2}{\mathrm{p}_{\mathcal{S}_0}(z)}.$$

Squared-Ratio Method: The Idea (1)

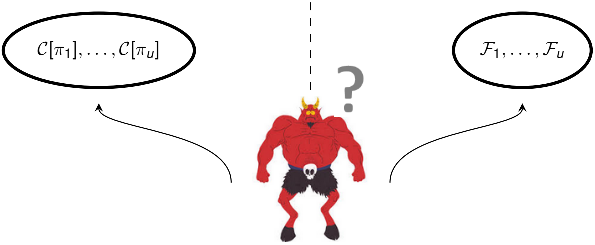


attacker $\mathcal{A}$

- $\mathcal{A}$ is allowed to make $q_{\max}$ 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 (1)



attacker $\mathcal{A}$

- $\mathcal{A}$ is allowed to make $q_{\max}$ 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 (2)

- This auxiliary relation enables us to get:

$$\Delta_{KL}\left(\mathrm{p}_{\mathcal{S}_1}(\cdot), \mathrm{p}_{\mathcal{S}_0}(\cdot)\right) \leq \sum_{j=1}^{u} \Delta_{KL}\left(\mathrm{p}_{\mathcal{S}_{1,j}}(\cdot), \mathrm{p}_{\mathcal{S}_{0,j}}(\cdot)\right)$$

- KL divergences for the multi-user security bound can be written as a summation of single-user security bounds

- It is sufficient to bound the KL divergence for a single user to prove multi-user security

Squared-Ratio Method:The Idea (2)

- This auxiliary relation enables us to get:

$$\Delta_{KL}\left(p_{\mathcal{S}_1}(\cdot), p_{\mathcal{S}_0}(\cdot)\right) \leq \sum_{j=1}^{u} \Delta_{KL}\left(p_{\mathcal{S}_{1,j}}(\cdot), p_{\mathcal{S}_{0,j}}(\cdot)\right)$$

- KL divergences for the multi-user security bound can be written as a summation of single-user security bounds

- It is sufficient to bound the KL divergence for a single user to prove multi-user security

Squared-Ratio Method:The Idea (2)

- This auxiliary relation enables us to get:

$$\Delta_{KL}\left(\mathrm{p}_{\mathcal{S}_1}(\cdot), \mathrm{p}_{\mathcal{S}_0}(\cdot)\right) \leq \sum_{j=1}^{u} \Delta_{KL}\left(\mathrm{p}_{\mathcal{S}_{1,j}}(\cdot), \mathrm{p}_{\mathcal{S}_{0,j}}(\cdot)\right)$$

- KL divergences for the multi-user security bound can be written as a summation of single-user security bounds

- It is sufficient to bound the KL divergence for a single user to prove multi-user security

Patarin's H-coefficient Technique

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

$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + \Pr[Z_{\mathcal{S}_0^1} \in \mathcal{T}_{\text{bad}}]$$

- $\mathcal{T}_{\text{bad}}$ and ϵ: depend on the construction
- $\Pr[Z_{\mathcal{S}_0^1} \in \mathcal{T}_{\text{bad}}]$: a combinatorial problem relies on the randomness in the ideal world

But We Want...

- We aim to prove that

$$\frac{P_{S_1,1}(z)}{P_{S_0,1}(z)} \leq 1 + \epsilon$$

- Combining it with the ratio in H-coefficient Technique, it holds that

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

- THE SQUARED-RATIO METHOD:

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

But We Want...

- We aim to prove that

$$\frac{P_{S_1,1}(z)}{P_{S_0,1}(z)} \leq 1 + \epsilon$$

- Combining it with the ratio in H-coefficient Technique, it holds that

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

- THE SQUARED-RATIO METHOD:

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

But We Want...

- We aim to prove that

$$\frac{P_{S_1,1}(z)}{P_{S_0,1}(z)} \leq 1 + \epsilon$$

- Combining it with the ratio in H-coefficient Technique, it holds that

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

- THE SQUARED-RATIO METHOD:

$$\|\mathsf{p}_{\mathcal{S}_1}(\cdot) - \mathsf{p}_{\mathcal{S}_0}(\cdot)\| \leq \sqrt{2u} \cdot \epsilon + 2u \cdot \Pr[Z_{\mathcal{S}_0} \in \mathcal{T}_{\text{bad}}]$$

System of Equations

- Two sets of unknown $\mathcal{P} = \{P_1, \ldots, P_{q_P}\}$ and $\mathcal{Q} = \{Q_1, \ldots, Q_{q_Q}\}$ and knowns values $\lambda_1, \ldots, \lambda_q$
- A system of equations

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

where φ_P and φ_Q are two surjective index mappings such that

$$\varphi_P \colon \{1, \ldots, q\} \to \{1, \ldots, q_P\},$$
$$\varphi_Q \colon \{1, \ldots, q\} \to \{1, \ldots, q_Q\},$$

- 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

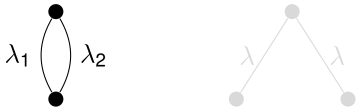
- Transcript graph should be
  - acyclic
  - non-zero path label (non-degenerate)

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)

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)



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)

Upper Bounds from Mirror Theory

- Previous Mirror theory can give a sharp “lower” bound of good transcripts z:

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

- Our new variant of Mirror theory gives both lower and upper bounds:

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

for some $\epsilon' \approx \epsilon$

Upper Bounds from Mirror Theory

- Previous Mirror theory can give a sharp “lower” bound of good transcripts z:

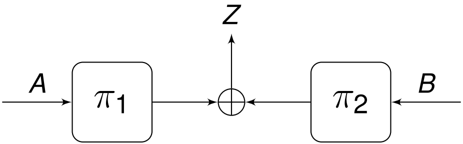
$$\frac{P_{S_1,1}(z)}{P_{S_0,1}(z)} \geq 1 - \epsilon$$

- Our new variant of Mirror theory gives both lower and upper bounds:

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

for some $\epsilon' \approx \epsilon$

Framework For Use

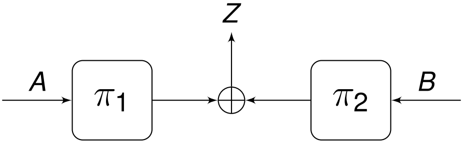


- Query transcript $\tau = \{(A_1, B_1, Z_1), \ldots, (A_q, B_q, Z_q)\}$
- Each such algorithm consists of an evaluation of π_1 and an evaluation of π_2

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

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

Framework For Use

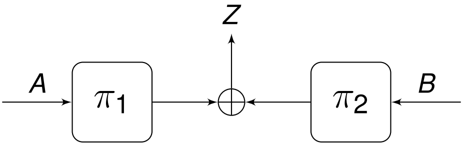


- Query transcript $\tau = \{(A_1, B_1, Z_1), \ldots, (A_q, B_q, Z_q)\}$
- Each such algorithm consists of an evaluation of π_1 and an evaluation of π_2

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

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

Framework For Use

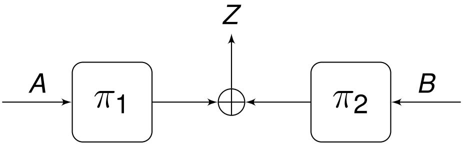


- Query transcript $\tau = \{(A_1, B_1, Z_1), \ldots, (A_q, B_q, Z_q)\}$
- Each such algorithm consists of an evaluation of π_1 and an evaluation of π_2

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

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

Framework For Use

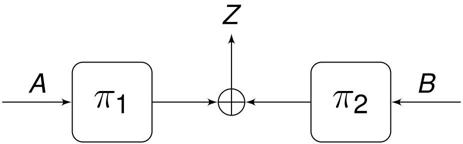


- Query transcript $\tau = \{(A_1, B_1, Z_1), \ldots, (A_q, B_q, Z_q)\}$
- Each such algorithm consists of an evaluation of π_1 and an evaluation of π_2

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

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

Framework For Use

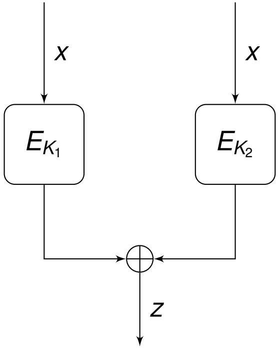


- Query transcript $\tau = \{(A_1, B_1, Z_1), \ldots, (A_q, B_q, Z_q)\}$
- Each such algorithm consists of an evaluation of π_1 and an evaluation of π_2

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

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

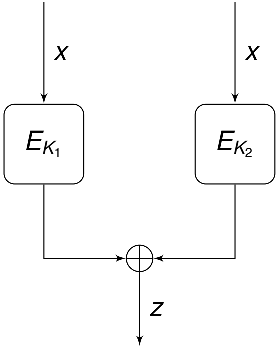
Application on Multi-User Security of XoP (1)



Bellare et al. (EC'89)
and Hall et al. (CR'89)

Paper	Bound	Security Level
Lucks '00	$\frac{q^3}{2^{2n}}$	$2^{2n/3}$
DHT '17	$\frac{q^{1.5}}{2^{1.5n}}$	2^n
DNS '22	$\frac{q^2}{2^{2n}}$	2^n

Application on Multi-User Security of XoP (2)



Bellare et al. (EC'89) and Hall et al. (CR'89)

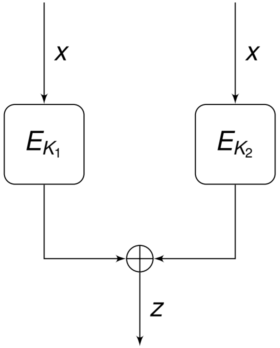
- CKLL (AC'21) showed for the first time a multi-user security of $O(\sqrt{u}{q_{\max}}^{1.5}/2^{1.5n})$
- Squared-ratio method:

$$\mathbf{Adv}^{\text{mu-prf}}_{\text{SoP}} \le O\left(\frac{\sqrt{u}{q_{\max}}^2}{2^{2n}}\right)$$

- Probably the optimal result as a generic reduction:

$$\mathbf{Adv}^{\text{mu-prf}}_{\text{SoP}}(u, q_{\max}) = O\left(\sqrt{u} \cdot \mathbf{Adv}^{\text{su-prf}}_{\text{SoP}}(q_{\max})\right)$$

Application on Multi-User Security of XoP (2)



Bellare et al. (EC'89) and Hall et al. (CR'89)

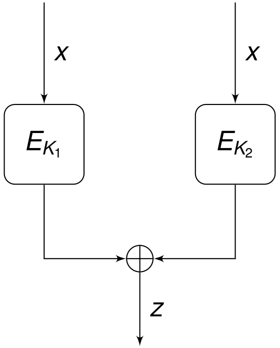
- CKLL (AC'21) showed for the first time a multi-user security of $O(\sqrt{u}{q_{max}}^{1.5}/2^{1.5n})$
- Squared-ratio method:

$$\mathbf{Adv}^{\text{mu-prf}}_{\text{SoP}} \leq O\left(\frac{\sqrt{u}{q_{max}}^2}{2^{2n}}\right)$$

- Probably the optimal result as a generic reduction:

$$\mathbf{Adv}^{\text{mu-prf}}_{\text{SoP}}(u, q_{max}) = O\left(\sqrt{u} \cdot \mathbf{Adv}^{\text{su-prf}}_{\text{SoP}}(q_{max})\right)$$

Application on Multi-User Security of XoP (2)



Bellare et al. (EC'89) and Hall et al. (CR'89)

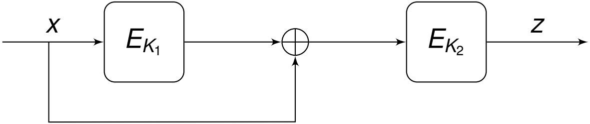
- CKLL (AC'21) showed for the first time a multi-user security of $O(\sqrt{u}{q_{\max}}^{1.5}/2^{1.5n})$
- Squared-ratio method:

$$\mathbf{Adv}_{\mathrm{SoP}}^{\text{mu-prf}} \leq O\left(\frac{\sqrt{u}{q_{\max}}^2}{2^{2n}}\right)$$

- Probably the optimal result as a generic reduction:

$$\mathbf{Adv}_{\mathrm{SoP}}^{\text{mu-prf}}(u, q_{\max}) = O\left(\sqrt{u} \cdot \mathbf{Adv}_{\mathrm{SoP}}^{\text{su-prf}}(q_{\max})\right)$$

Application on Multi-User Security of EDM

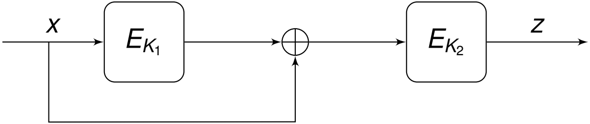


Cogliati and Seurin (CR'16)

- Cogliati and Seurin proved single-user security up to $O(2^{\frac{2n}{3}})$
- Best known multi-user security bound is $O\left(uq^2/2^{1.5n}\right) \rightarrow$ combination of hybrid argument with the result of DNT (CR'17)
- Squared-ratio method:

$$\mathbf{Adv}^{\text{mu-prf}}_{\text{EDM}} \leq O\left(\frac{n\sqrt{u}q_{\max}{}^{4}}{2^{3n}}\right)$$

Application on Multi-User Security of EDM

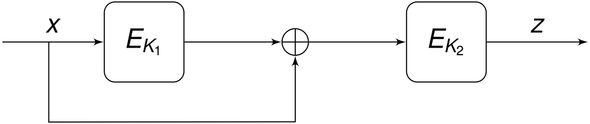


Cogliati and Seurin (CR'16)

- Cogliati and Seurin proved single-user security up to $O(2^{\frac{2n}{3}})$
- Best known multi-user security bound is $O\left(uq^2/2^{1.5n}\right) \rightarrow$ combination of hybrid argument with the result of DNT (CR'17)
- Squared-ratio method:

$$\mathbf{Adv}^{\text{mu-prf}}_{\text{EDM}} \leq O\left(\frac{n\sqrt{u}{q_{\max}}^4}{2^{3n}}\right)$$

Application on Multi-User Security of EDM

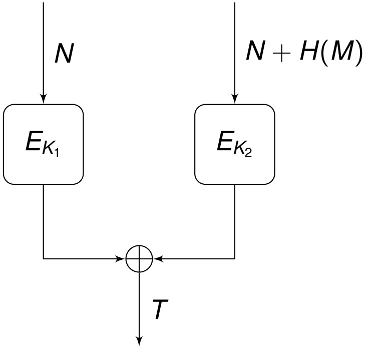


Cogliati and Seurin (CR'16)

- Cogliati and Seurin proved single-user security up to $O(2^{\frac{2n}{3}})$
- Best known multi-user security bound is $O\left(uq^2/2^{1.5n}\right) \rightarrow$ combination of hybrid argument with the result of DNT (CR'17)
- Squared-ratio method:

$$\mathbf{Adv}^{\text{mu-prf}}_{\text{EDM}} \leq O\left(\frac{n\sqrt{u}{q_{\max}}^4}{2^{3n}}\right)$$

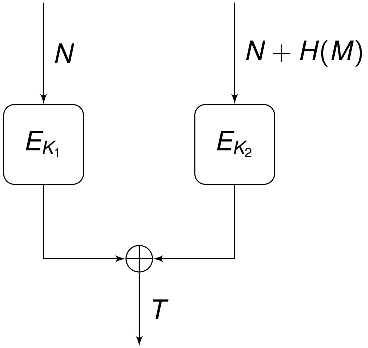
Application on Multi-User Security of nEHTM (1)



DNS (EC'19)

- Two permutation variant = $F^{\mathrm{SoP}}_{B_2}$ construction by CMP (AC'21)
- DNS (EC'19) proved single-user security up to $O(2^{2n/3})$
- CLLL (AC'20) improved the single-user security to $O(2^{3n/4})$
- Single permutation case has a naive and tight advantage bound $uq_{\max}/2^n$
- Squared-ratio method: improved multi-user security for nonce-respecting setting

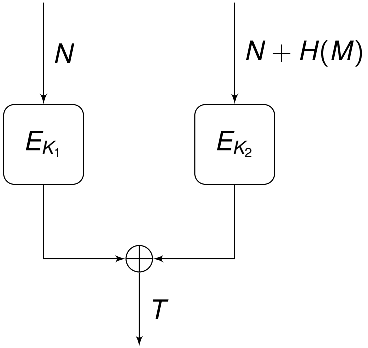
Application on Multi-User Security of nEHTM (1)



DNS (EC'19)

- Two permutation variant = $F^{\text{SoP}}_{B_2}$ construction by CMP (AC'21)
- DNS (EC'19) proved single-user security up to $O(2^{2n/3})$
- CLLL (AC'20) improved the single-user security to $O(2^{3n/4})$
- Single permutation case has a naive and tight advantage bound $uq_{\max}/2^n$
- Squared-ratio method: improved multi-user security for nonce-respecting setting

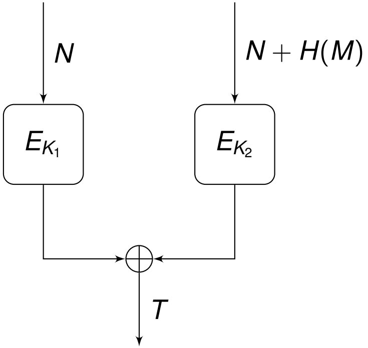
Application on Multi-User Security of nEHTM (1)



DNS (EC'19)

- Two permutation variant = $F^{\text{SoP}}_{B_2}$ construction by CMP (AC'21)
- DNS (EC'19) proved single-user security up to $O(2^{2n/3})$
- CLLL (AC'20) improved the single-user security to $O(2^{3n/4})$
- Single permutation case has a naive and tight advantage bound $uq_{\max}/2^n$
- Squared-ratio method: improved multi-user security for nonce-respecting setting

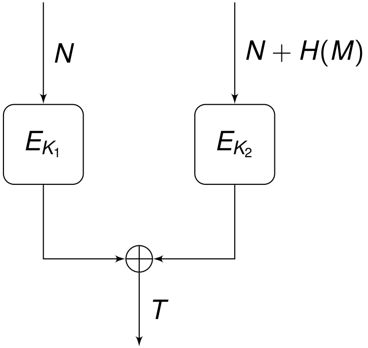
Application on Multi-User Security of nEHTM (1)



DNS (EC'19)

- Two permutation variant = $F^{\mathrm{SoP}}_{B_2}$ construction by CMP (AC'21)
- DNS (EC'19) proved single-user security up to $O(2^{2n/3})$
- CLLL (AC'20) improved the single-user security to $O(2^{3n/4})$
- Single permutation case has a naive and tight advantage bound $uq_{\max}/2^n$
- Squared-ratio method: improved multi-user security for nonce-respecting setting

Application on Multi-User Security of nEHTM (1)

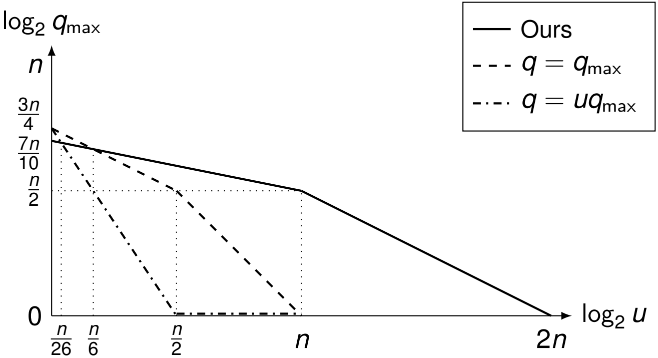


DNS (EC'19)

- Two permutation variant = $F^{\text{SoP}}_{B_2}$ construction by CMP (AC'21)
- DNS (EC'19) proved single-user security up to $O(2^{2n/3})$
- CLLL (AC'20) improved the single-user security to $O(2^{3n/4})$
- Single permutation case has a naive and tight advantage bound $uq_{\text{max}}/2^n$
- Squared-ratio method: improved multi-user security for nonce-respecting setting

Application on Multi-User Security of nEHTM (2)

- Our bound is superior for $u \geq O\left(2^{\frac{n}{26}}\right)$ and $2^{\frac{n}{26}} \approx 30.3$ if $n = 128$ and $q = uq_{\max}$.



Conclusion

New results

- Squared-Ratio method
- Upper bound for mirror theory
- Improved multi-user security of XoP, EDM, and nEHtM

Future research

- Apply Squared-Ratio method to more difficult constructions
- Improving mirror theory
- Other modular proof techniques for multi-user security proofs

Thank you for your attention!

Conclusion

New results

- Squared-Ratio method
- Upper bound for mirror theory
- Improved multi-user security of XoP, EDM, and nEHtM

Future research

- Apply Squared-Ratio method to more difficult constructions
- Improving mirror theory
- Other modular proof techniques for multi-user security proofs

Thank you for your attention!

Conclusion

New results

- Squared-Ratio method
- Upper bound for mirror theory
- Improved multi-user security of XoP, EDM, and nEHtM

Future research

- Apply Squared-Ratio method to more difficult constructions
- Improving mirror theory
- Other modular proof techniques for multi-user security proofs

Thank you for your attention!

The End