Information Bounds and Convergence Rates for Side-Channel Security Evaluators

Loïc Masure **Gaëtan Cassiers** Julien Hendrickx
François-Xavier Standaert

Table of Contents

Content

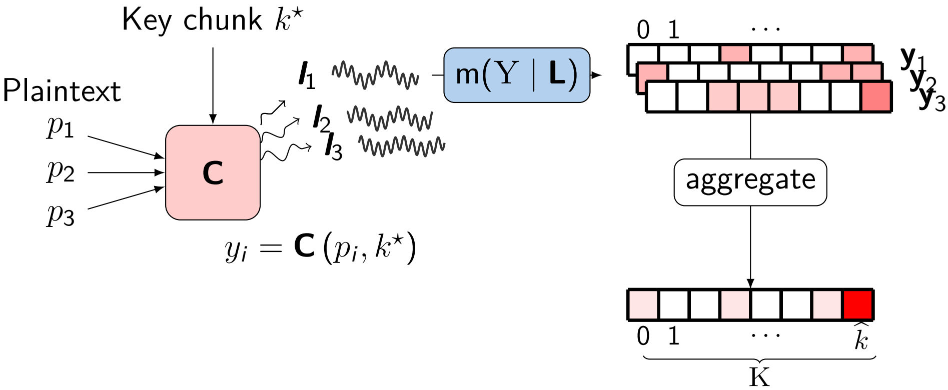
Leakage certification

State-of-the art

A discussion of eHI

New Metrics

Profiled SCA



Information-based Leakage Certification

What is the minimal number of traces $N_a^\star$ needed for the best adversary to succeed with proba. $\geq \beta$?

Information-based Leakage Certification

What is the minimal number of traces $N_a^\star$ needed for the best adversary to succeed with proba. $\geq \beta$?

MI bound [dCGRP19]:

$$N_a^\star \geq \frac{f(\beta)}{\mathrm{MI}(\mathrm{Y}; \mathbf{L})}$$

Information-based Leakage Certification

What is the minimal number of traces $N_a^\star$ needed for the best adversary to succeed with proba. $\geq \beta$?

MI bound [dCGRP19]:

$$N_a^\star \geq \frac{f(\beta)}{\mathrm{MI}(\mathrm{Y}; \mathbf{L})}$$

How can we bound $\mathrm{MI}(\mathbf{Y}; \mathbf{L})$?

Problem parameters

- Y: target intermediate variable, n-bit (uniform)
- $\mathbf{L}$: leakage trace: continuous $\mathbb{R}^D$ or discrete $\{0,1\}^{\omega D}$ sampling
- $\mathrm{m}(\mathrm{Y} \mid \mathbf{L})$: profiled model, approximates true distribution $\mathrm{p}(\mathrm{Y} \mid \mathbf{L})$
- $\mathcal{S}_a$: set of attack traces, $N_a = |\mathcal{S}_a|$
- $\mathcal{S}_p$: set of profiling traces, $N_p = |\mathcal{S}_p|$

Content

Leakage certification

State-of-the art

A discussion of eHI

New Metrics

MI lower bound

Mutual information formula:

$$\mathsf{MI}(\mathrm{Y};\mathbf{L}) = \mathsf{H}(\mathrm{Y}) + \mathop{\mathbb{E}}_{y,\boldsymbol{l}} \log_2 \left(\Pr\left(\mathrm{Y}=y \mid \mathbf{L}=\boldsymbol{l}\right)\right)$$

MI lower bound

Mutual information formula:

$$\mathsf{MI}\left(\mathrm{Y};\mathbf{L}\right)=\mathsf{H}(\mathrm{Y})+\mathop{\mathbb{E}}_{y,\boldsymbol{l}}\log_2\left(\Pr\left(\mathrm{Y}=y\mid\mathbf{L}=\boldsymbol{l}\right)\right)$$

We can use different models m, m′:

$$\Delta_{\mathsf{m}}^{\mathsf{m}'}=\mathsf{H}(\mathrm{Y})+\sum_{y,\boldsymbol{l}}\mathsf{m}(\boldsymbol{l},y)\log_2\left(\mathsf{m}'(y\mid\boldsymbol{l})\right)\qquad\qquad \mathsf{MI}\left(\mathrm{Y};\mathbf{L}\right)=\Delta_{\mathsf{p}}^{\mathsf{p}}$$

MI lower bound

Mutual information formula:

$$\mathsf{MI}(Y;\mathbf{L}) = \mathsf{H}(Y) + \mathop{\mathbb{E}}_{y,\boldsymbol{l}} \log_2\left(\Pr\left(Y = y \mid \mathbf{L} = \boldsymbol{l}\right)\right)$$

We can use different models m, m′:

$$\Delta_{\mathsf{m}}^{\mathsf{m}'} = \mathsf{H}(Y) + \sum_{y,\boldsymbol{l}} \mathsf{m}(\boldsymbol{l}, y) \log_2\left(\mathsf{m}'(y \mid \boldsymbol{l})\right) \qquad \mathsf{MI}(Y;\mathbf{L}) = \Delta_{\mathsf{p}}^{\mathsf{p}}$$

Perceived Information (PI) [RSV+11,BHM+19]:

$$\mathsf{PI}_{\mathsf{m}'}(Y;\mathbf{L}) = \Delta_{\mathsf{p}}^{\mathsf{m}'}$$

$$\mathsf{PI}_{\mathsf{m}'}(Y;\mathbf{L}) \leq \mathsf{MI}(Y;\mathbf{L})$$

MI lower bound

Mutual information formula:

$$\mathrm{MI}(Y;\mathbf{L}) = \mathrm{H}(Y) + \mathop{\mathbb{E}}_{y,\boldsymbol{l}} \log_2 \left(\Pr\left(Y = y \mid \mathbf{L} = \boldsymbol{l}\right)\right)$$

We can use different models m, m′:

$$\Delta_{\mathrm{m}}^{\mathrm{m}'} = \mathrm{H}(Y) + \sum_{y,\boldsymbol{l}} \mathrm{m}(\boldsymbol{l}, y) \log_2 \left(\mathrm{m}'(y \mid \boldsymbol{l})\right) \qquad \mathrm{MI}(Y;\mathbf{L}) = \Delta_{\mathrm{p}}^{\mathrm{p}}$$

Perceived Information (PI) [RSV+11,BHM+19]:

$$\mathrm{PI}_{\mathrm{m}'}(Y;\mathbf{L}) = \Delta_{\mathrm{p}}^{\mathrm{m}'} \qquad \widehat{\mathrm{PI}}_{\mathrm{m}'}(Y;\mathbf{L}) = \Delta_{\tilde{\mathrm{e}}_{\mathcal{S}_v}}^{\mathrm{m}'}$$

$$\mathrm{PI}_{\mathrm{m}'}(Y;\mathbf{L}) \leq \mathrm{MI}(Y;\mathbf{L}) \qquad \mathbb{E}\left[\widehat{\mathrm{PI}}_{\mathrm{m}'}(Y;\mathbf{L})\right] \leq \mathrm{MI}(Y;\mathbf{L})$$

MI upper bound [BHM+19]

Hypothetical information (HI):

$$\mathsf{HI}_{\mathsf{m}'}(\mathrm{Y};\mathrm{L}) = \Delta_{\mathsf{m}'}^{\mathsf{m}'}$$

MI upper bound [BHM+19]

Hypothetical information (HI):

$$\mathsf{HI}_{\mathsf{m}'}(\mathrm{Y};\mathrm{L}) = \Delta_{\mathsf{m}'}^{\mathsf{m}'}$$

Empirical HI:

$$\mathsf{eHI}_{N_p}(\mathrm{Y};\mathbf{L}) = \mathsf{HI}_{\tilde{\mathsf{e}}_{\mathcal{S}_p}}(\mathrm{Y};\mathbf{L})$$

$$\mathbb{E}\left[\mathsf{eHI}_{N_p}(\mathrm{Y};\mathbf{L})\right] \geq \mathsf{MI}(\mathrm{Y};\mathbf{L})$$

MI upper bound [BHM+19]

Hypothetical information (HI):

$$\mathsf{HI}_{\mathsf{m'}}(\mathrm{Y};\mathrm{L}) = \Delta_{\mathsf{m'}}^{\mathsf{m'}}$$

Empirical HI:

$$\mathsf{eHI}_{N_p}(\mathrm{Y};\mathbf{L}) = \mathsf{HI}_{\tilde{\mathsf{e}}_{\mathcal{S}_p}}(\mathrm{Y};\mathbf{L})$$

$$\mathbb{E}\left[\mathsf{eHI}_{N_p}(\mathrm{Y};\mathbf{L})\right] \geq \mathsf{MI}(\mathrm{Y};\mathbf{L})$$

How many traces N_p are required to get tight bounds?

Content

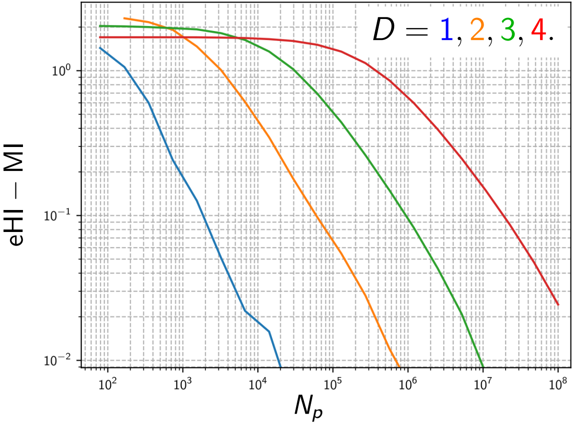
Profiling Complexity

Trace acquisition campaign: often the critical task ($\approx$ several days)...

Profiling Complexity

Trace acquisition campaign: often the critical task (≈ several days)...

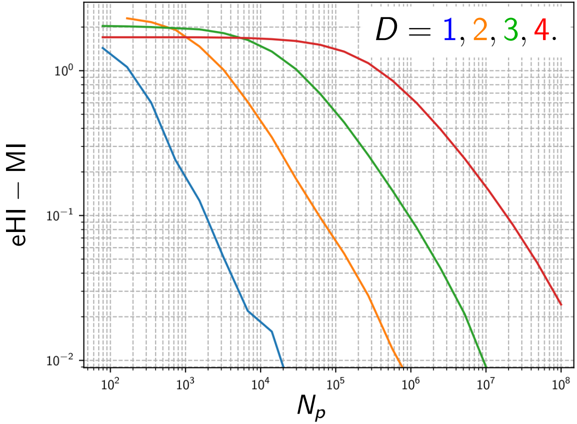
...but convergence of eHI is **exponentially slow**.



Profiling Complexity

Trace acquisition campaign: often the critical task ($\approx$ several days)...

...but convergence of eHI is **exponentially slow**.



a.k.a. *curse of dimensionality*

Root cause: $\log(\tilde{e}_{\mathcal{S}_p})$

Not an issue for PI.

Non-empirical HI?

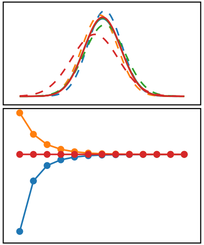
Simulation setting:

- 2-bit masked variable: $\mathbf{L} = \mathrm{HW}(x_0, x_1, y_0, y_1) + N$, $\mathrm{Y} = (x_0 \oplus x_1, y_0 \oplus y_1)$.
- Gaussian templates

Non-empirical HI?

Simulation setting:

- 2-bit masked variable: $\mathbf{L} = \mathrm{HW}(x_0, x_1, y_0, y_1) + N$, $\mathrm{Y} = (x_0 \oplus x_1, y_0 \oplus y_1)$.
- Gaussian templates



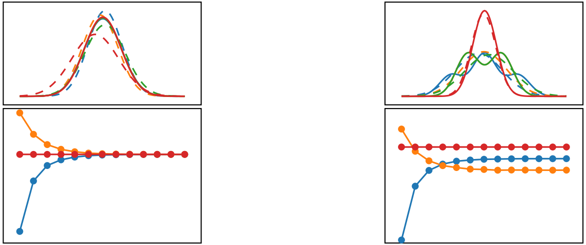
$\mathrm{SNR} = 0.02$

PI, HI and MI vs. N_p

Non-empirical HI?

Simulation setting:

- 2-bit masked variable: $\mathbf{L} = \mathrm{HW}(x_0, x_1, y_0, y_1) + N$, $\mathrm{Y} = (x_0 \oplus x_1, y_0 \oplus y_1)$.
- Gaussian templates



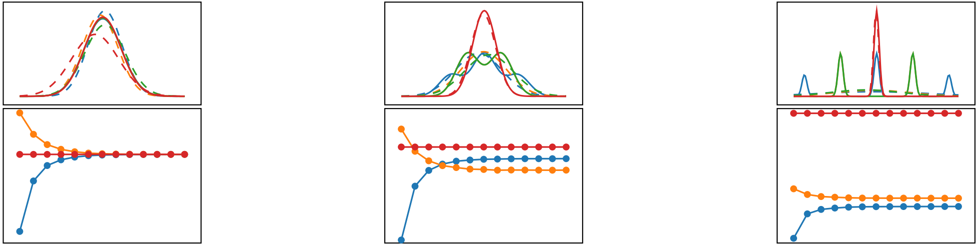
$\mathrm{SNR} = 0.02$ $\mathrm{SNR} = 2$

PI, HI and MI vs. N_p

Non-empirical HI?

Simulation setting:

- 2-bit masked variable: $\mathbf{L} = \mathrm{HW}(x_0, x_1, y_0, y_1) + N$, $\mathrm{Y} = (x_0 \oplus x_1, y_0 \oplus y_1)$.
- Gaussian templates



$\mathrm{SNR} = 0.02$ $\mathrm{SNR} = 2$ $\mathrm{SNR} = 200$

PI, HI and MI vs. N_p

Content

Towards New Evaluation Metrics

Additional assumptions:

- Restrict the adversary to a collection $\mathcal{H}$ of models
  - E.g., Gaussian templates, neural networks...
- The adversary selects the best model from $\mathcal{H}$.

Towards New Evaluation Metrics

Additional assumptions:

- Restrict the adversary to a collection $\mathcal{H}$ of models
  - E.g., Gaussian templates, neural networks...
- The adversary selects the best model from $\mathcal{H}$.

New metric: LI

$$\mathsf{LI}_{\mathcal{H}}(\mathrm{Y};\mathbf{L}) = \sup_{\mathsf{m}\in\mathcal{H}} \mathsf{PI}_{\mathsf{m}}(\mathrm{Y};\mathbf{L}) \leq \mathsf{MI}(\mathrm{Y};\mathbf{L})$$

Towards New Evaluation Metrics

Additional assumptions:

- Restrict the adversary to a collection $\mathcal{H}$ of models
  - E.g., Gaussian templates, neural networks...
- The adversary selects the best model from $\mathcal{H}$.

New metric: LI

$$\mathsf{LI}_{\mathcal{H}}(\mathrm{Y};\mathbf{L}) = \sup_{\mathsf{m}\in\mathcal{H}} \mathsf{PI}_{\mathsf{m}}(\mathrm{Y};\mathbf{L}) \leq \mathsf{MI}(\mathrm{Y};\mathbf{L})$$

Surrogate to MI: $\mathsf{PI}(\mathrm{Y};\mathbf{L}) \leq \mathsf{LI}_{\mathcal{H}}(\mathrm{Y};\mathbf{L}) \leq \mathsf{MI}(\mathrm{Y};\mathbf{L})$ (still bounds N_a)

What about an upper bound to LI?

Upper Bound to LI

Natural adversarial strategy: maximize $\mathsf{PI}_{\mathsf{m}}(Y; \mathbf{L}) = \Delta_{\mathsf{p}}^{\mathsf{m}}$.

Upper Bound to LI

Natural adversarial strategy: maximize $\mathsf{PI}_\mathsf{m}(Y; \mathbf{L}) = \Delta_\mathsf{p}^\mathsf{m}$.

Surrogate: maximize $\Delta_{\tilde{\mathsf{e}}_{\mathcal{S}_p}}^\mathsf{m}$.

Upper Bound to LI

Natural adversarial strategy: maximize $\mathsf{PI}_{\mathsf{m}}(\mathrm{Y}; \mathbf{L}) = \Delta_{\mathsf{p}}^{\mathsf{m}}$.

Surrogate: maximize $\Delta^{\mathsf{m}}_{\tilde{\mathsf{e}}_{\mathcal{S}_p}}$.

TI-maximizer

Any $\mathcal{H}$-adversary $\mathcal{A}_{\mathcal{H}}$ is a TI-maximizer iff

$$\mathcal{A}_{\mathcal{H}}(\tilde{\mathsf{e}}_{\mathcal{S}_p}) = \operatorname*{argmax}_{\mathsf{m}\in\mathcal{H}} \Delta^{\mathsf{m}}_{\tilde{\mathsf{e}}_{\mathcal{S}_p}} .$$

Upper Bound to LI

Natural adversarial strategy: maximize $\mathsf{PI}_{\mathsf{m}}(\mathrm{Y}; \mathbf{L}) = \Delta_{\mathsf{p}}^{\mathsf{m}}$.

Surrogate: maximize $\Delta_{\tilde{\mathsf{e}}_{\mathcal{S}_p}}^{\mathsf{m}}$.

TI-maximizer

Any $\mathcal{H}$-adversary $\mathcal{A}_{\mathcal{H}}$ is a TI-maximizer iff

$$\mathcal{A}_{\mathcal{H}}(\tilde{\mathsf{e}}_{\mathcal{S}_p}) = \operatorname*{argmax}_{\mathsf{m} \in \mathcal{H}} \Delta_{\tilde{\mathsf{e}}_{\mathcal{S}_p}}^{\mathsf{m}} .$$

Then, we denote

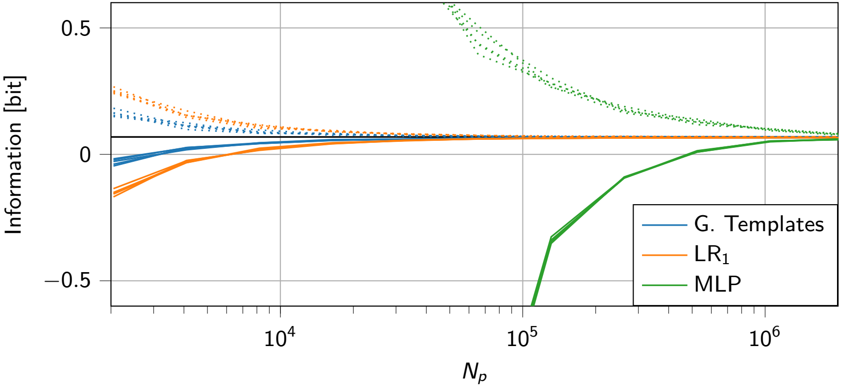
$$\mathsf{TI}_{N_p}(\mathrm{Y}; \mathbf{L}; \mathcal{A}_{\mathcal{H}}) = \Delta_{\tilde{\mathsf{e}}_{\mathcal{S}_p}}^{\mathcal{A}_{\mathcal{H}}(\tilde{\mathsf{e}}_{\mathcal{S}_p})} .$$

TI upper-bounds LI

$$\mathsf{PI}_{\mathsf{m}}\left(\mathrm{Y};\mathbf{L}\right) \leq \mathsf{LI}_{\mathcal{H}}\left(\mathrm{Y};\mathbf{L}\right) \leq \mathbb{E}\left[\mathsf{TI}_{N_p}\left(\mathrm{Y};\mathbf{L};\mathcal{A}_{\mathcal{H}}\right)\right]$$

TI upper-bounds LI

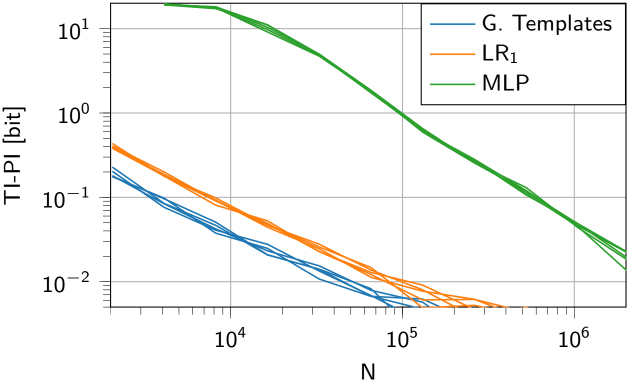
$$\mathsf{PI}_{\mathsf{m}}\left(Y;\mathbf{L}\right) \leq \mathsf{LI}_{\mathcal{H}}\left(Y;\mathbf{L}\right) \leq \mathbb{E}\left[\mathsf{TI}_{N_p}\left(Y;\mathbf{L};\mathcal{A}_{\mathcal{H}}\right)\right]$$



Dotted lines: TI. Solid lines: PI.

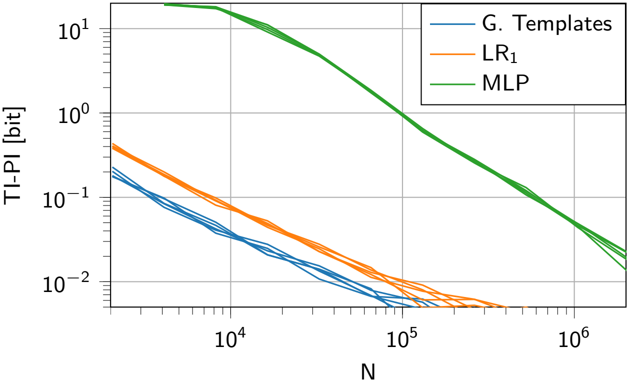
Convergence Rate

PI and TI converge to LI at a rate $\widetilde{\mathcal{O}}\left(\frac{poly(\mathcal{H})}{N_p}\right)$.



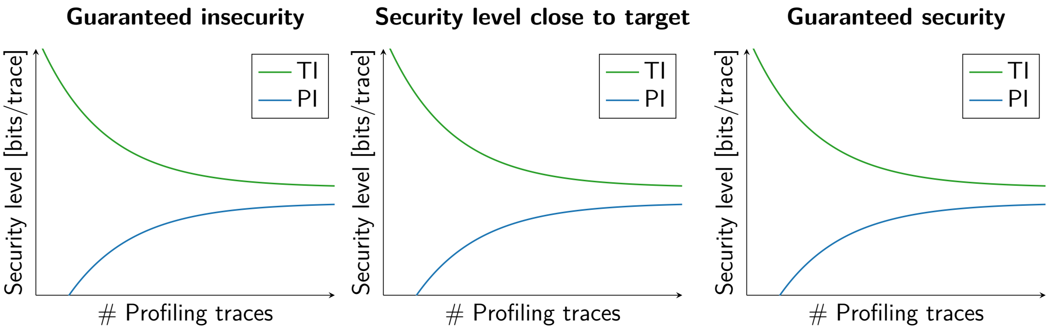
Convergence Rate

PI and TI converge to LI at a rate $\widetilde{\mathcal{O}}\left(\frac{poly(\mathcal{H})}{N_p}\right)$.



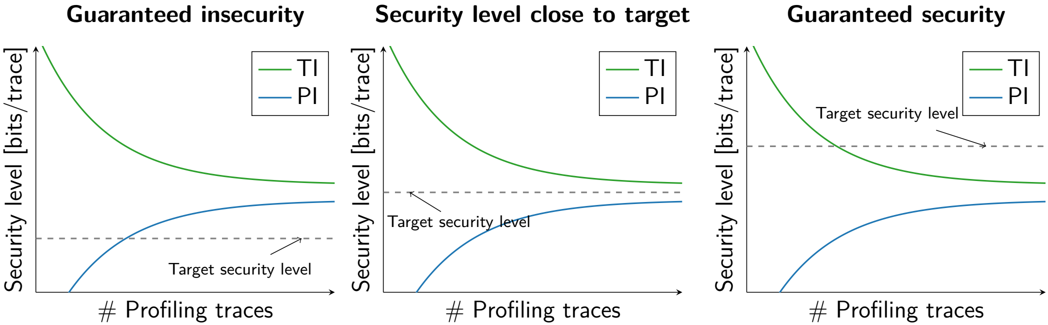
Predict required N_p to reach tightness goal.

Evaluation Outcomes



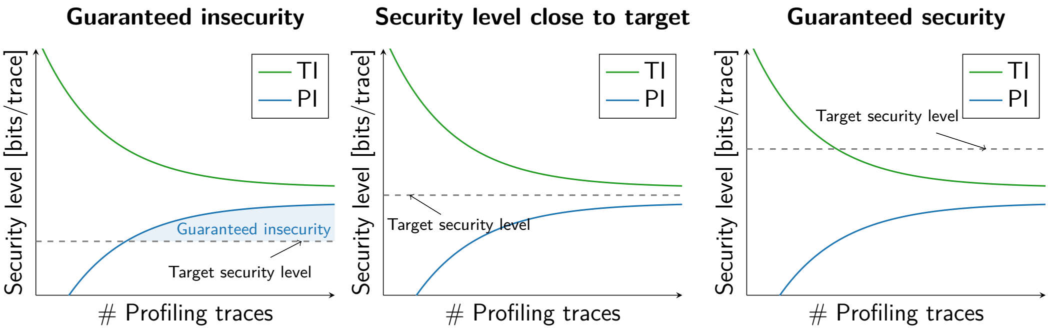
$\tilde{\mathcal{O}}\left(\frac{poly(\mathcal{H})}{N}\right)$ **convergence: no curse of dimensionality.**

Evaluation Outcomes



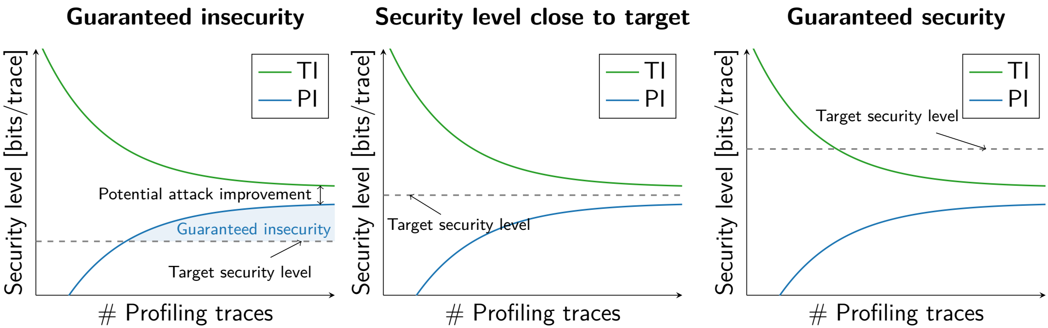
$\tilde{\mathcal{O}}\left(\frac{poly(\mathcal{H})}{N}\right)$ **convergence: no curse of dimensionality.**

Evaluation Outcomes



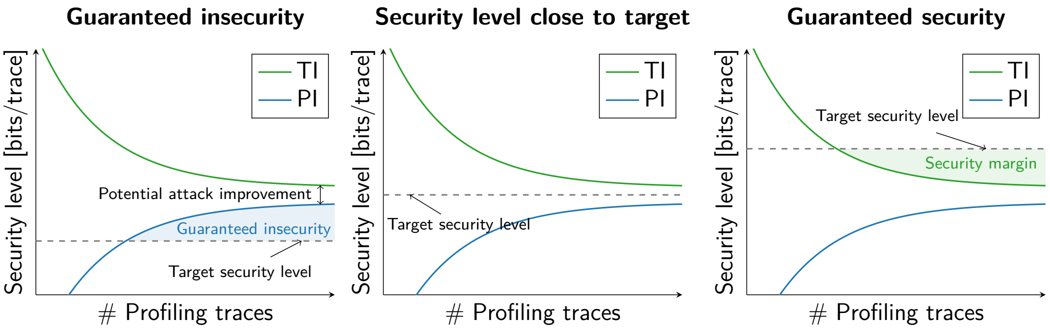
$\tilde{\mathcal{O}}\left(\frac{poly(\mathcal{H})}{N}\right)$ **convergence: no curse of dimensionality.**

Evaluation Outcomes



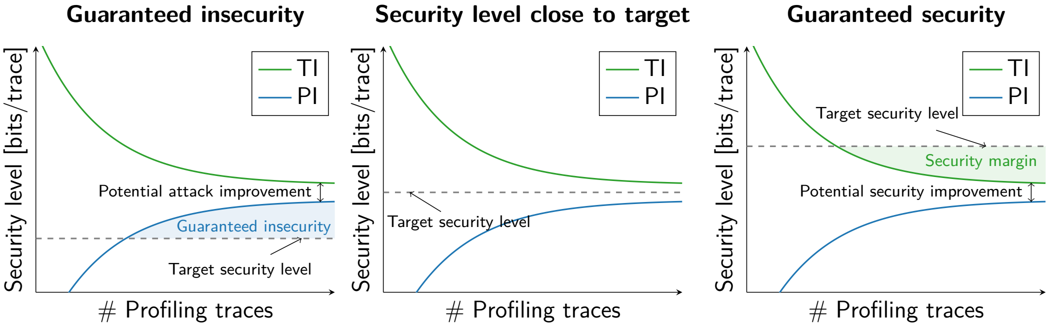
$\tilde{\mathcal{O}}\left(\frac{poly(\mathcal{H})}{N}\right)$ **convergence: no curse of dimensionality.**

Evaluation Outcomes



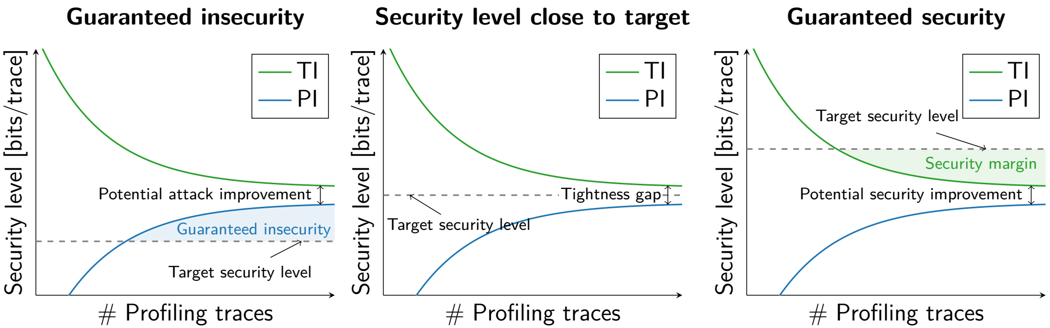
$\tilde{\mathcal{O}}\left(\frac{poly(\mathcal{H})}{N}\right)$ **convergence: no curse of dimensionality.**

Evaluation Outcomes



$\tilde{\mathcal{O}}\left(\frac{poly(\mathcal{H})}{N}\right)$ **convergence: no curse of dimensionality.**

Evaluation Outcomes



$\tilde{\mathcal{O}}\left(\frac{poly(\mathcal{H})}{N}\right)$ **convergence: no curse of dimensionality.**

Conclusion

- We provide to the Side-Chanel Analysis (SCA) evaluator some theoretical insights to assess the *profiling* complexity.
- Hypothetical Information (HI) can be replaced by a tighter metric: TI
  - TI converges to LI $\rightarrow$ bounds best *known* attack.
  - Fast convergence, scalable to highly multivariate leakage.
  - Loses connection to MI.