Metior

A Comprehensive Model To Evaluate Obfuscating Side-Channel Defense Schemes

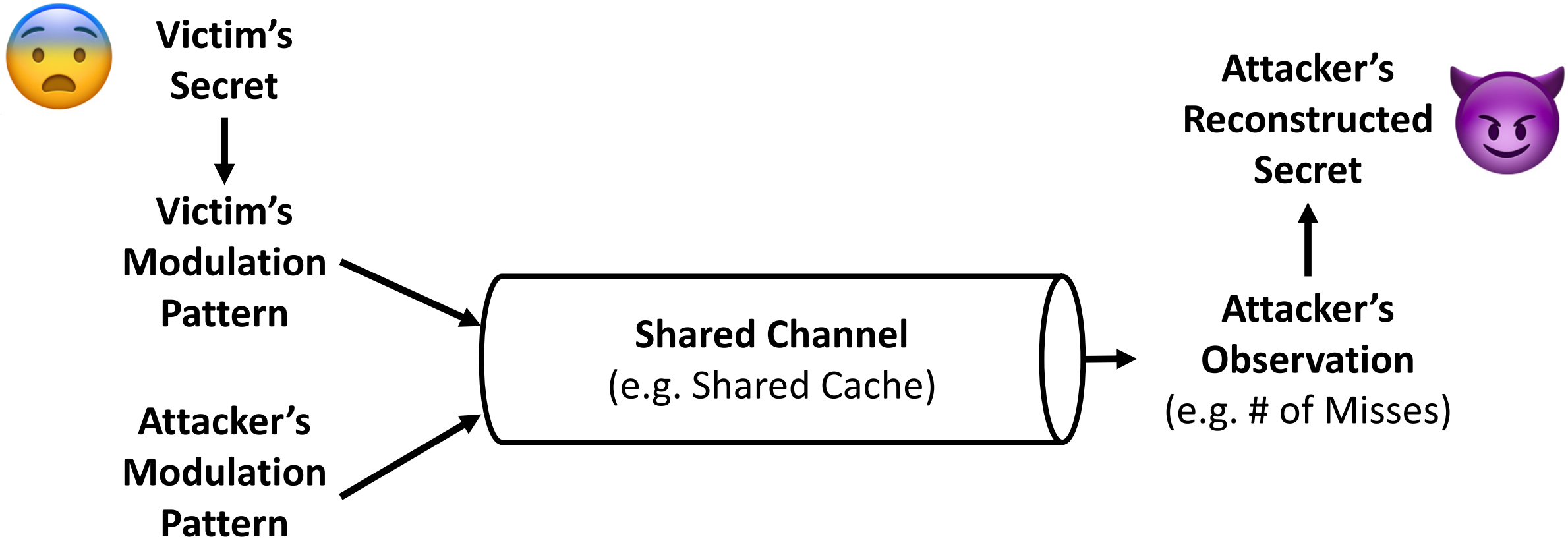
Peter W. Deutsch, Weon Taek Na, Thomas Bourgeat, Joel Emer*, and Mengjia Yan

MIT CSAIL, *MIT CSAIL/NVIDIA

ISCA 2023 - Session 1C

June 19th 2023

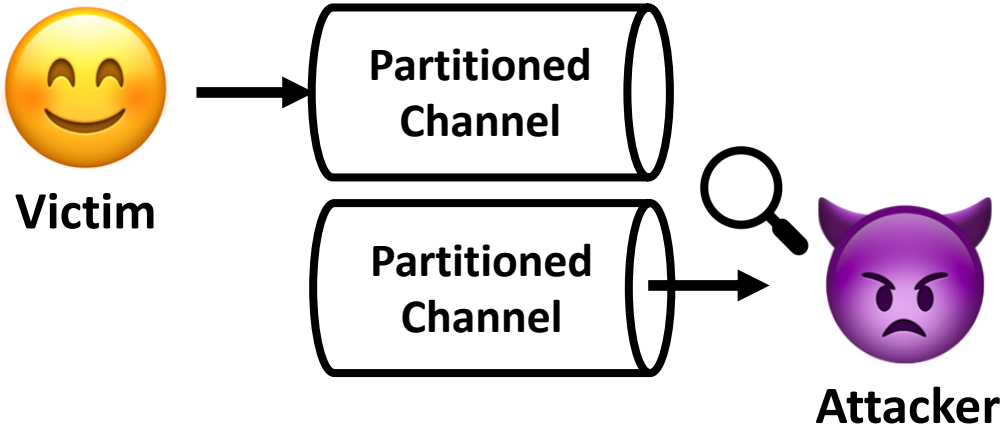
Side-Channel Overview



Side-Channel Defenses

Partitioning Defense Schemes

e.g. Cache Partitioning

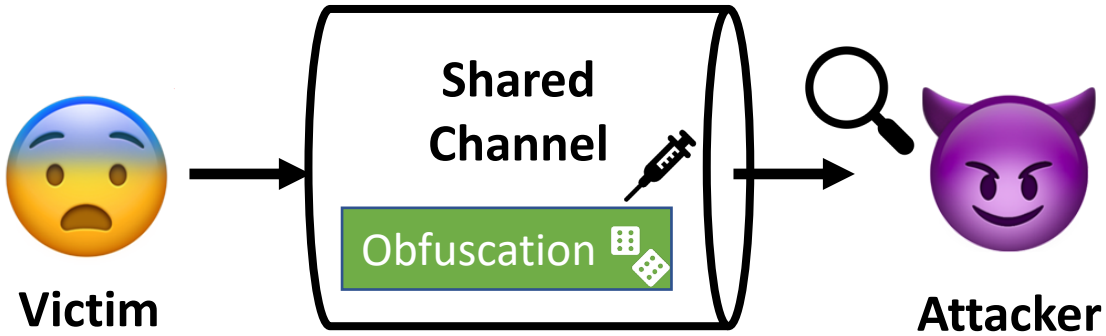


✓ ***Completely Block Leakage***

✗ ***Poor Performance***

Obfuscating Defense Schemes

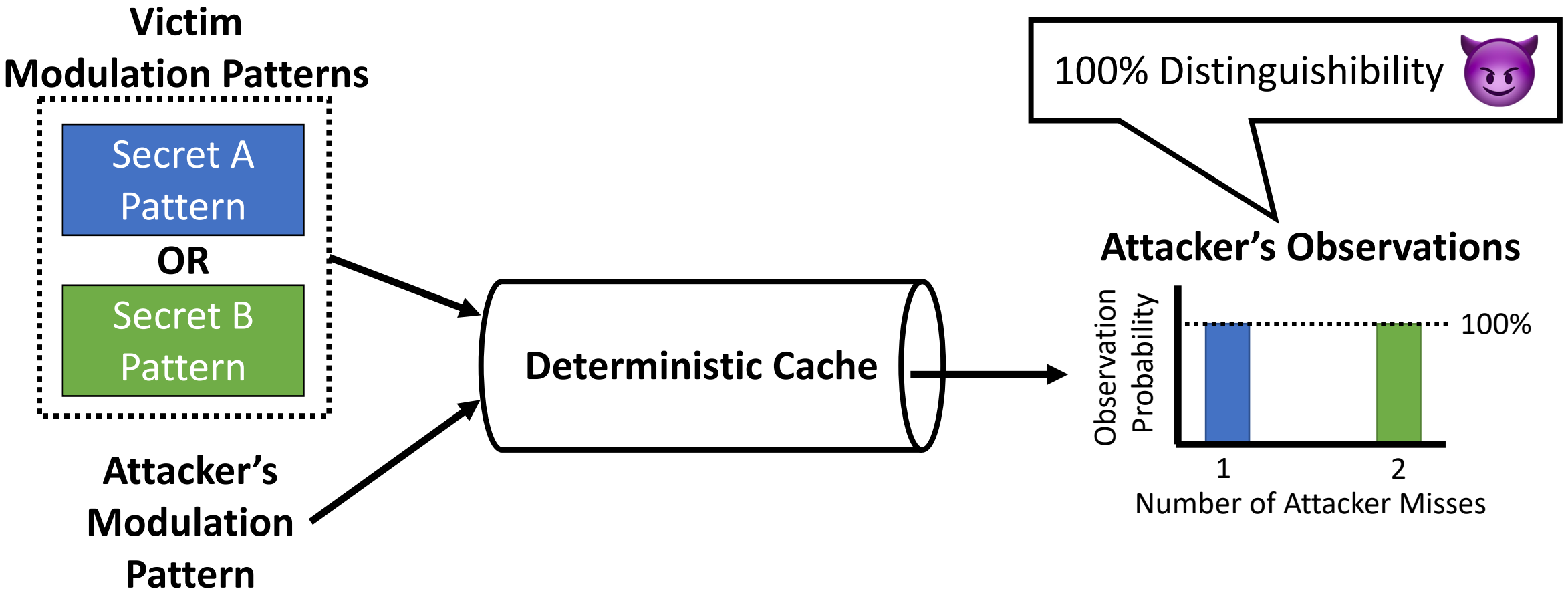
e.g. Randomized Caches, Traffic Shaping, Noise Injection



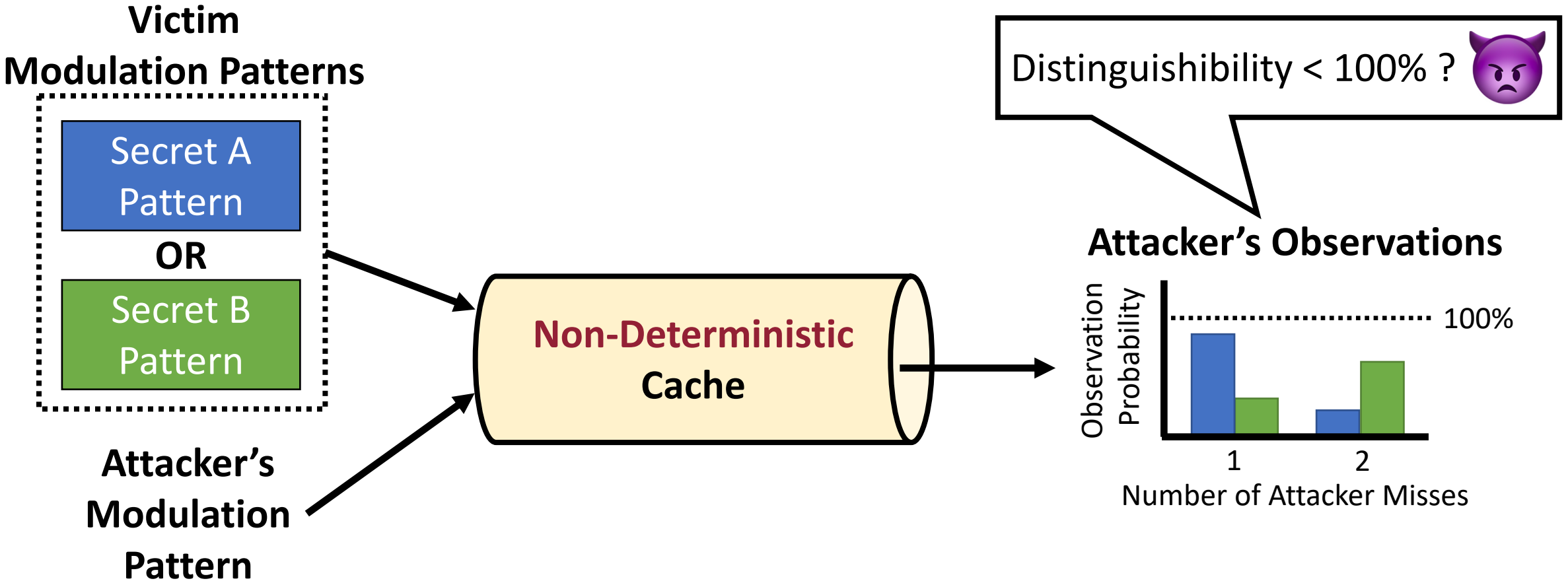
Unclear Leakage

✓ ***Reasonable Performance***

Analysis Example

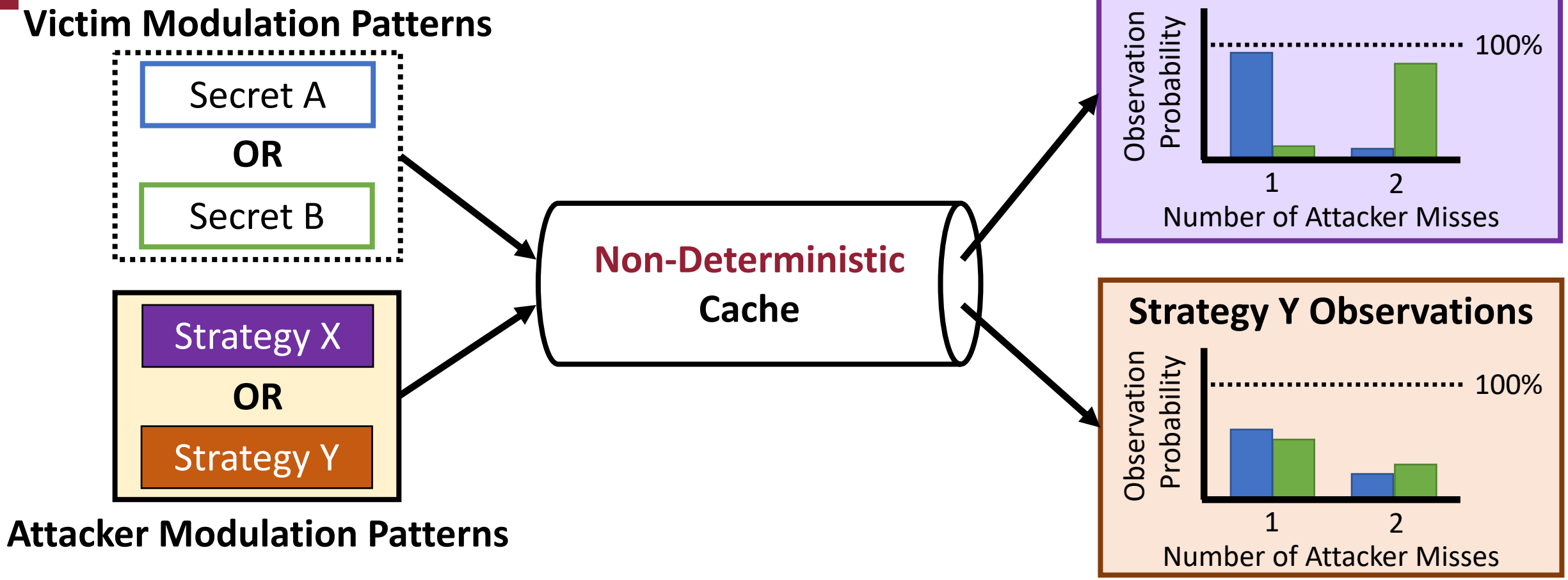


Analysis Example



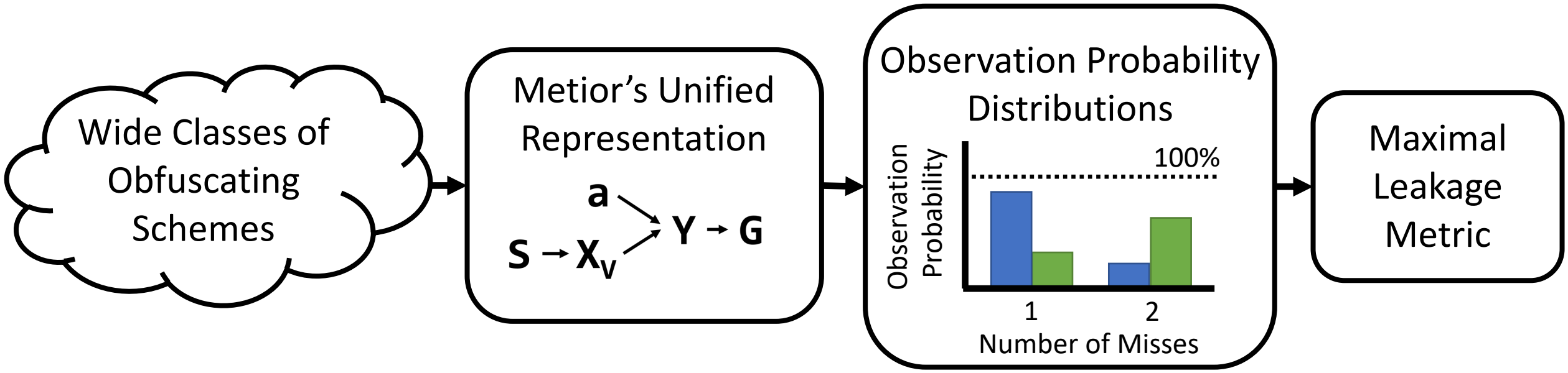
Does adding non-determinism increase security? If so, *by how much*?

What About the Attacker?



The attacker's strategy is critical in understanding leakage

Metior

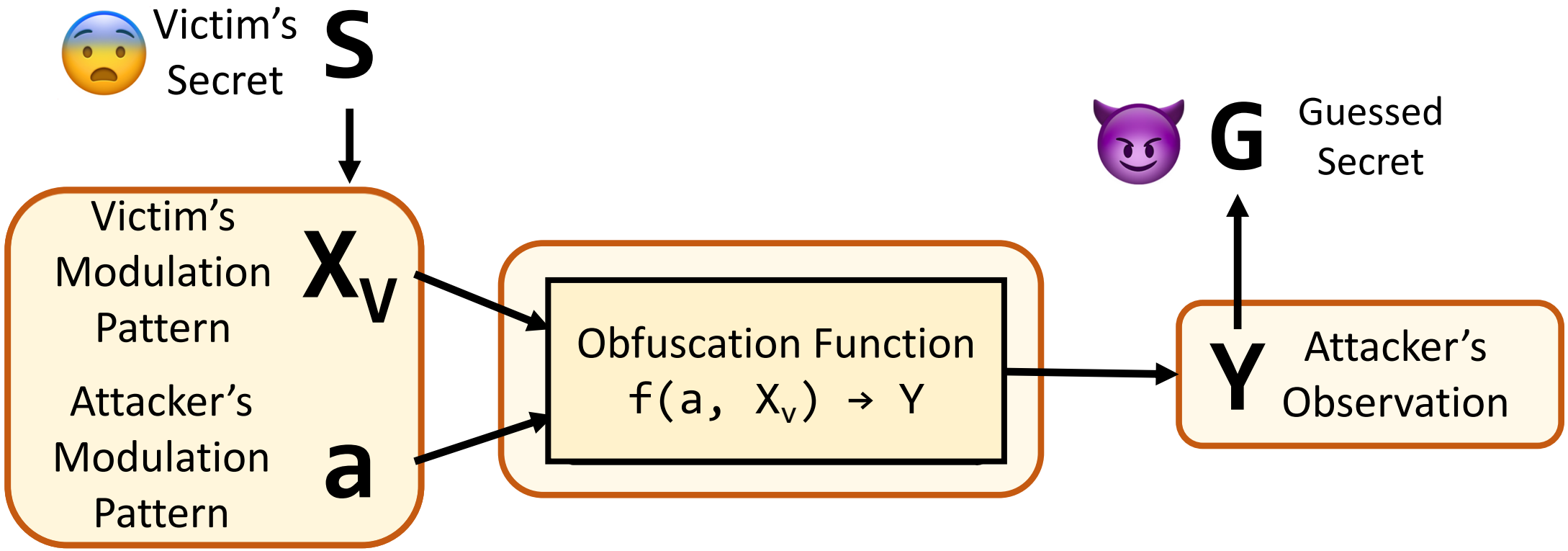


Prior Work: Customized modeling solutions for specific defenses and victims

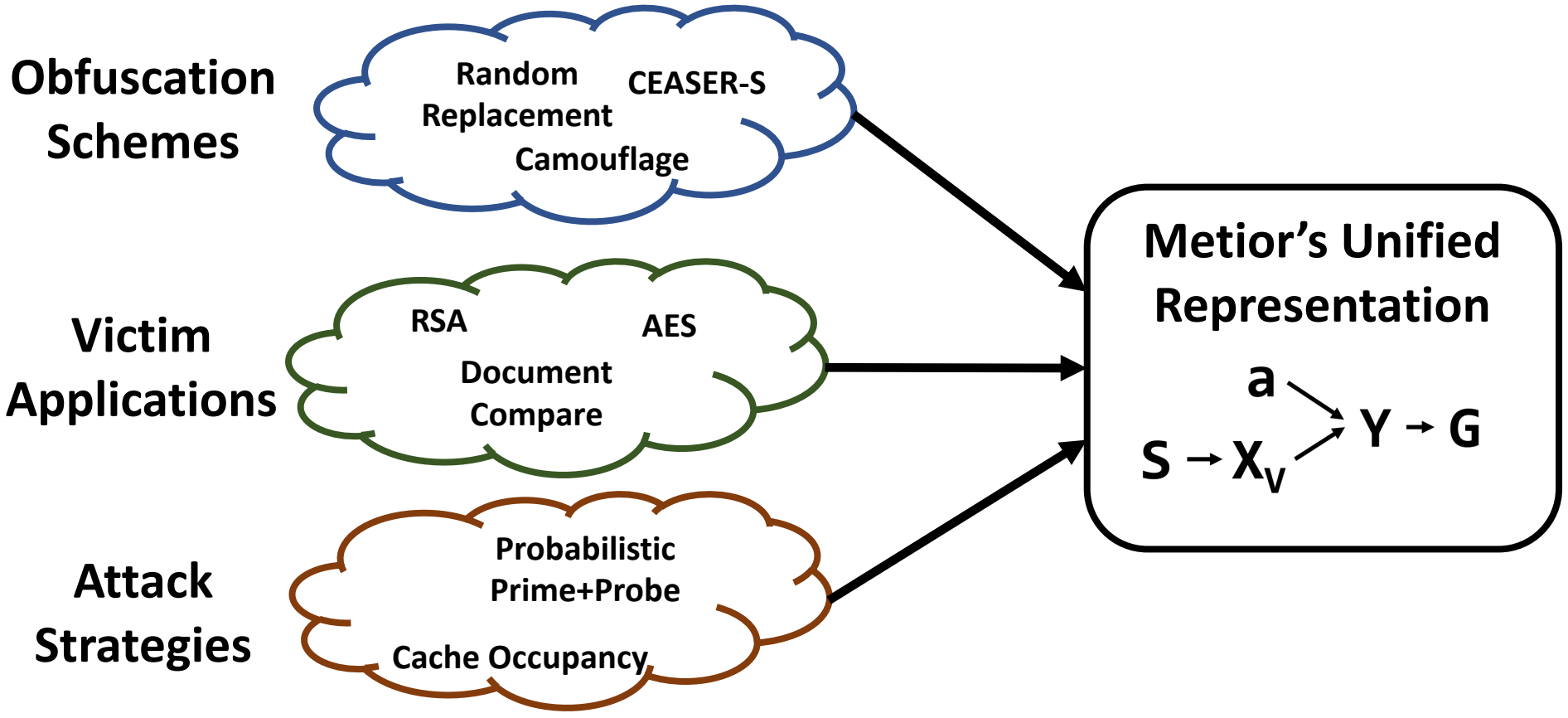
Metior's Goal: A unified solution for varying channels, victims, and attackers

Metior's Unified Representation

Obfuscated side-channels can be represented as *random variables* and the relationships between them!



Metior's Case Studies



Case Study – Randomly Mapped Caches

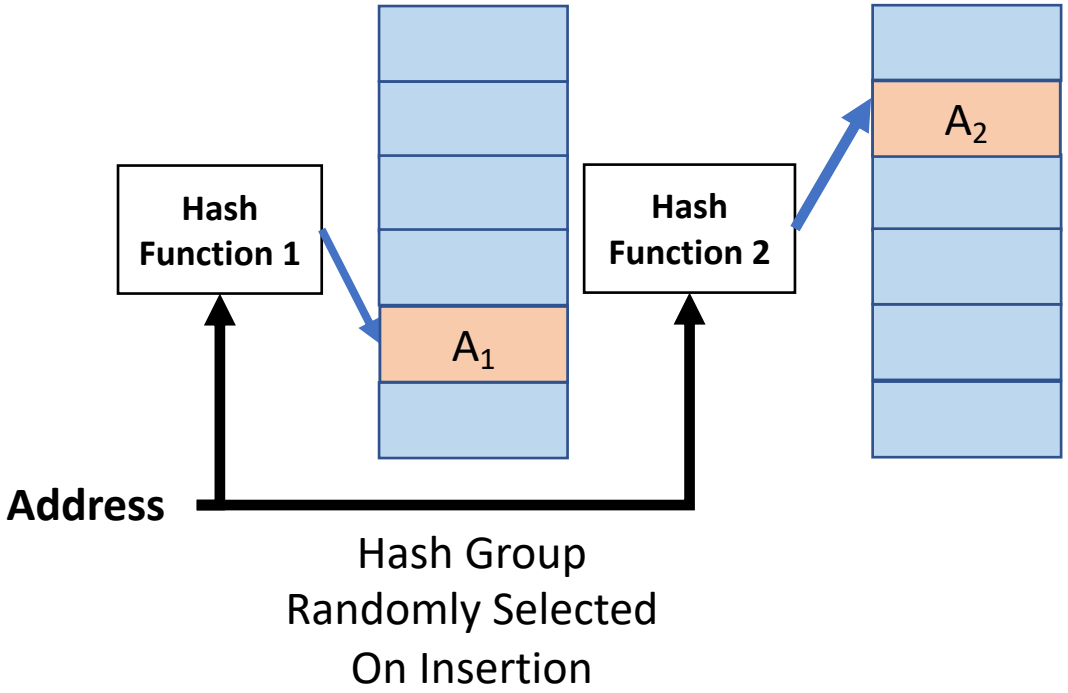
Using Metior, we can explore the leakage of state-of-the-art randomized caches.

In doing so, we are able to:

Better understand the *root causes* of leakage

Demonstrate the importance of studying *real victims*

Case Study – Types of Attacks



We study two attacks

① **Cache Occupancy**

Capacity Misses

Random Addresses → Prime + Probe

② **Probabilistic Prime + Probe (PPP)**

Targeted Set Conflicts

Calibration → Eviction Set → Prime + Probe

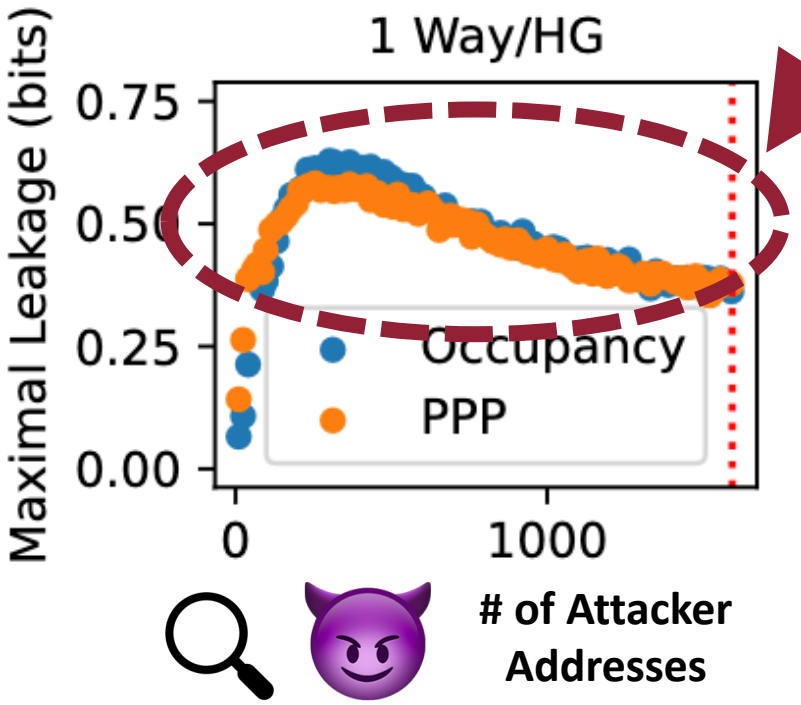
Leakage Expectation: PPP > Cache Occupancy

Case Study – Results

RSA Encryption Victim

Secret 0 → 10 Cache Accesses

Secret 1 → 26 Cache Accesses



Probabilistic P+P ≈ Cache Occupancy!

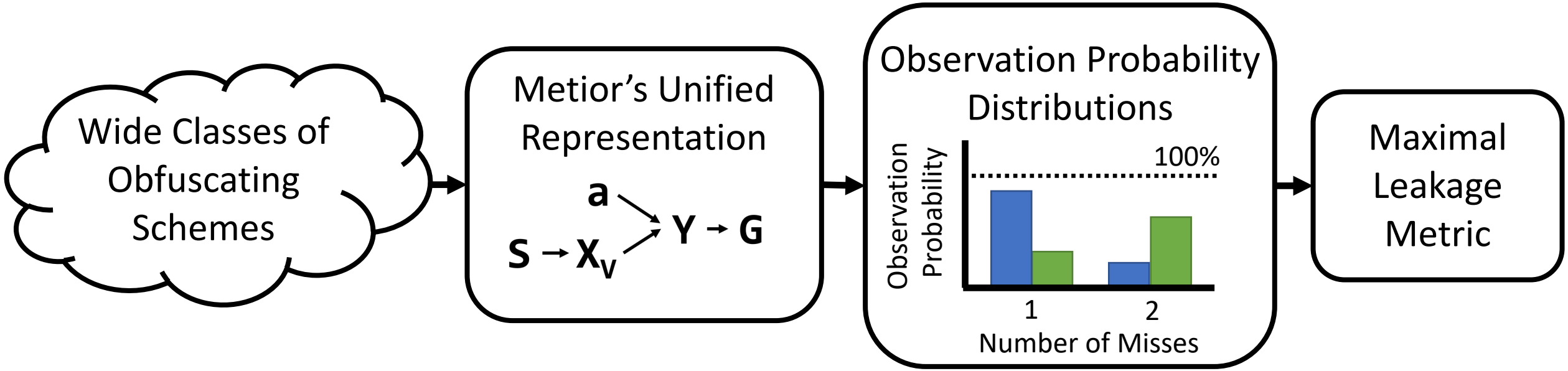
Takeaway #1

Metior helps in understanding the root cause of obfuscating scheme leakage

Takeaway #2

Mitigations should broadly consider different dimensions of victim modulation patterns

Metior's Key Contributions



① A <u>unified model</u> for representing and evaluating obfuscating defense schemes

② Multiple case studies revealing unintuitive insights into state-of-the-art victims, attacks, and defenses

Metior

A Comprehensive Model To Evaluate Obfuscating Side-Channel Defense Schemes

Peter W. Deutsch
pwd@mit.edu

Weon Taek Na
weontaek@mit.edu

Thomas Bourgeat
bthom@mit.edu

Joel S. Emer
jsemer@mit.edu

Mengjia Yan
mengjiay@mit.edu

MIT CSAIL
compute. collaborate. create