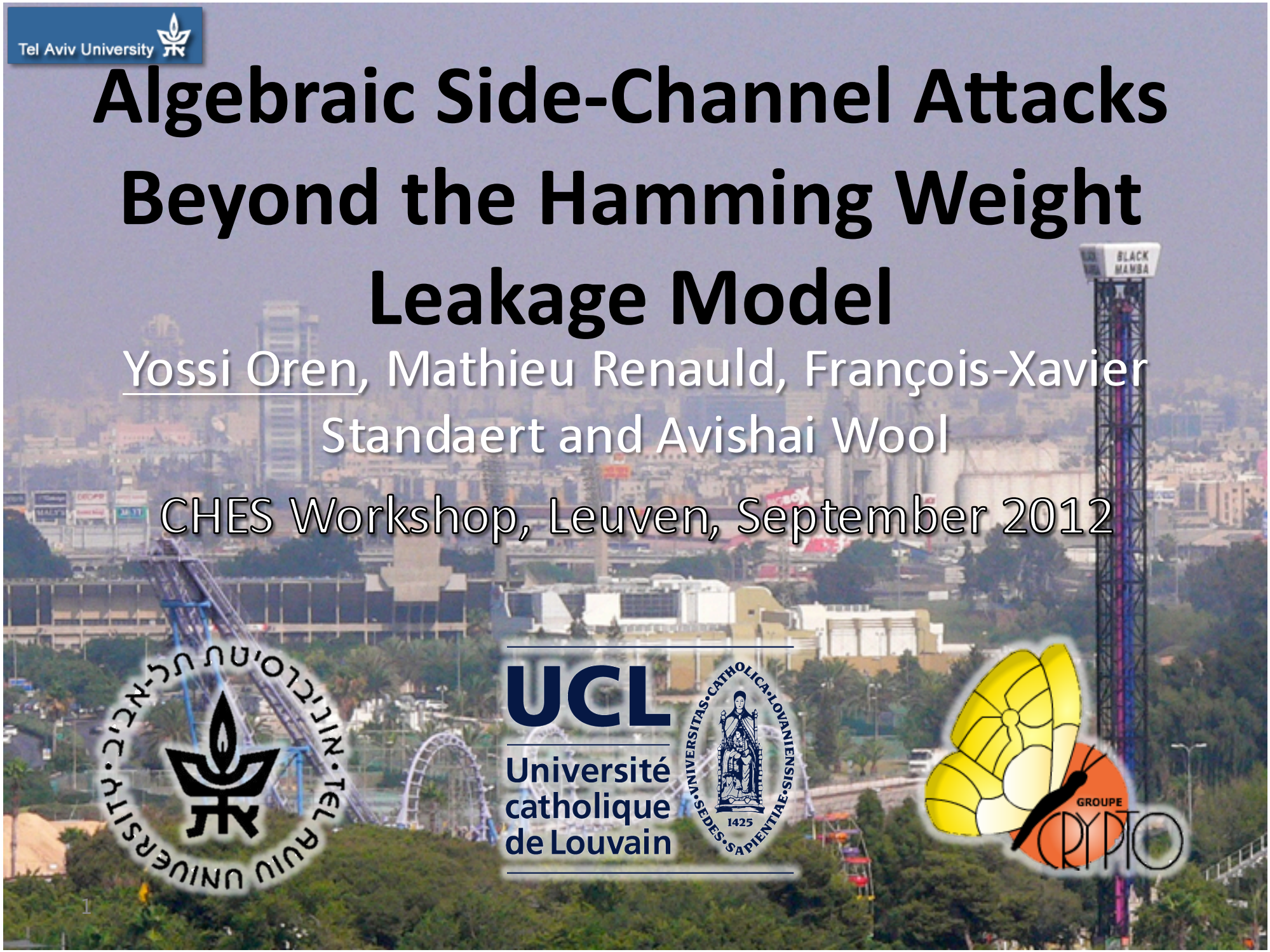


Algebraic Side-Channel Attacks Beyond the Hamming Weight Leakage Model

Yossi Oren, Mathieu Renauld, François-Xavier Standaert and Avishai Wool

CHES Workshop, Leuven, September 2012

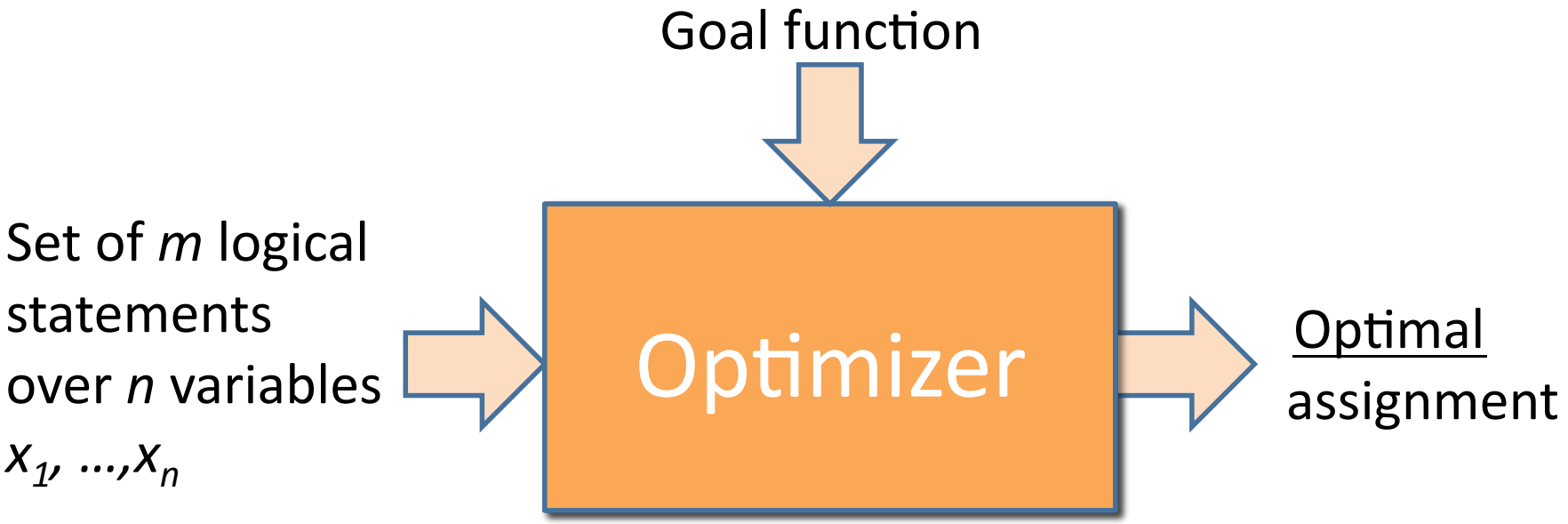
Tel Aviv University

Outline

- What is Template-TASCA?
- How do you use it?

Tel Aviv University

Review: solvers and optimizers



Tel Aviv University

Cryptanalysis using solvers

- Modern crypto is strong enough to withstand Algebraic Cryptanalysis using solvers [MM00]
- If we add side-channel inf… y can be recovered quickly and …
- Physical limitations of the… introduce errors which ca… by replacing solvers with opt…0]

Oren, Kirschbaum, Popp and Wool, CHES 2010

Renauld and Standaert, INSCRYPT 2009

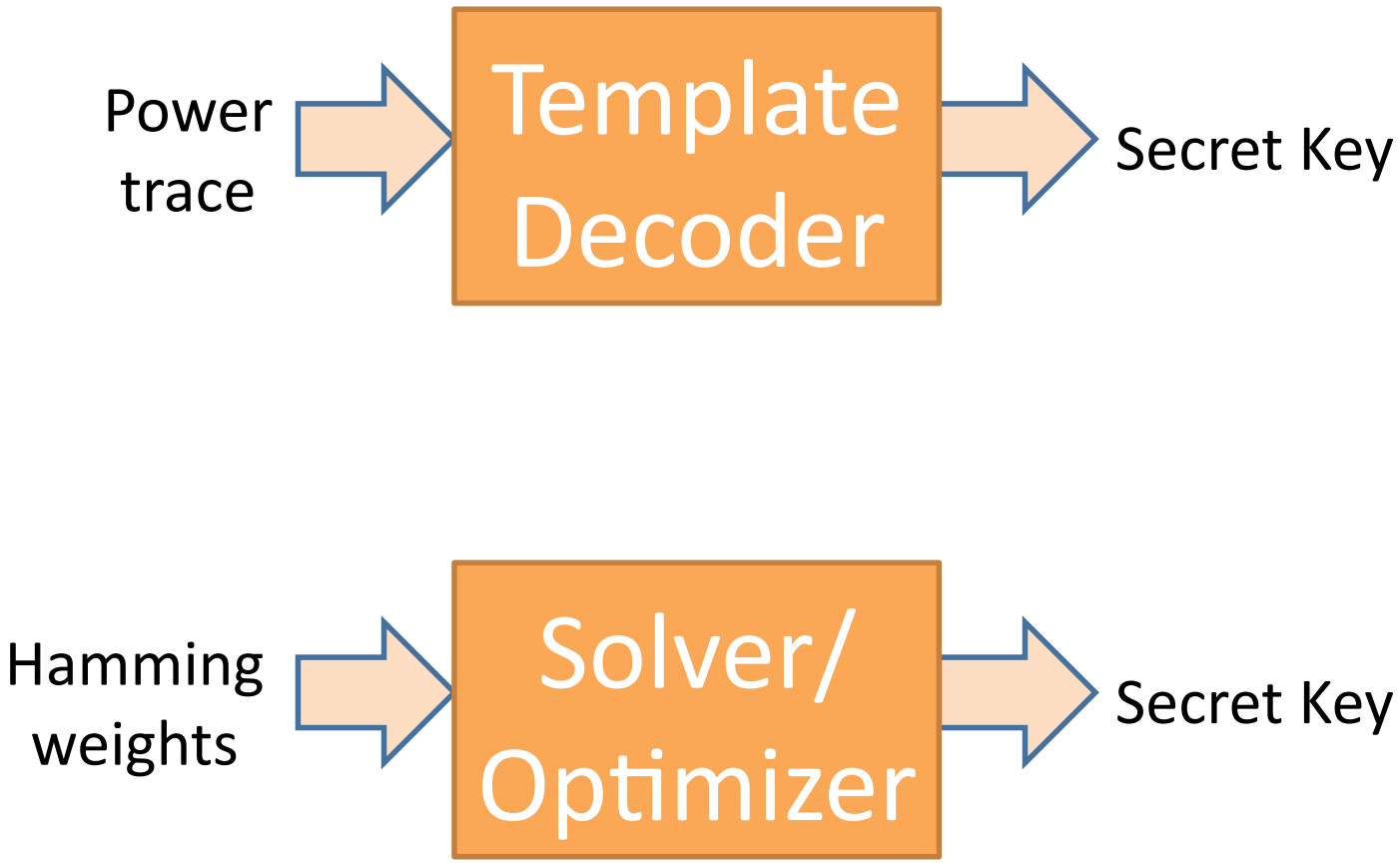
Tel Aviv University

Our contributions

- We extend ASCA from a priori (HW) leakage model towards **any profiled model**
- The resulting attack methodology, called Template-TASCA (alt. Template-Set-ASCA), combines the **low data complexity** of algebraic attacks and the **versatility** of template attacks
- Our results apply both to **solvers** and to **optimizers**

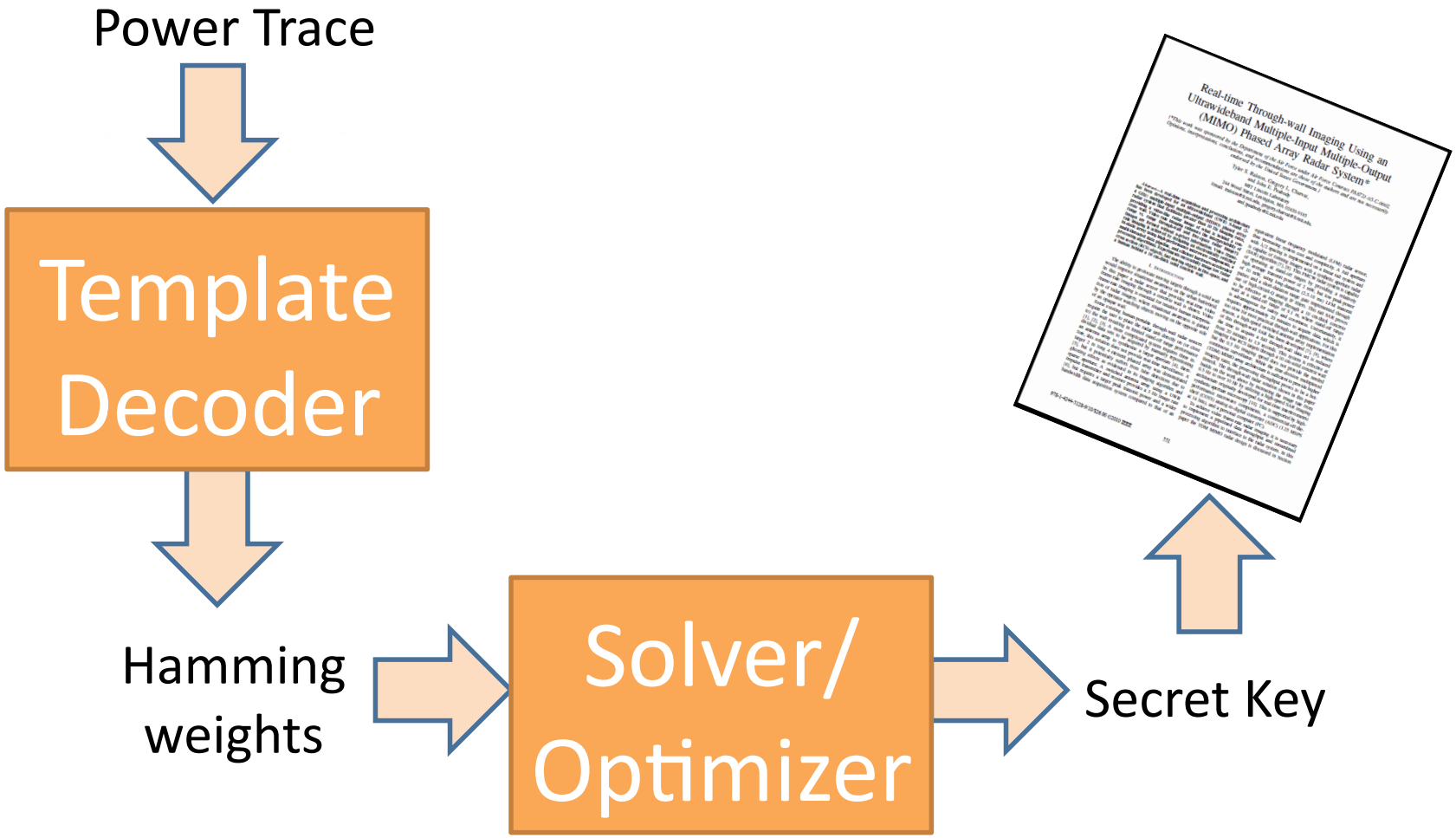
Tel Aviv University

Versatility of Template-TASCA



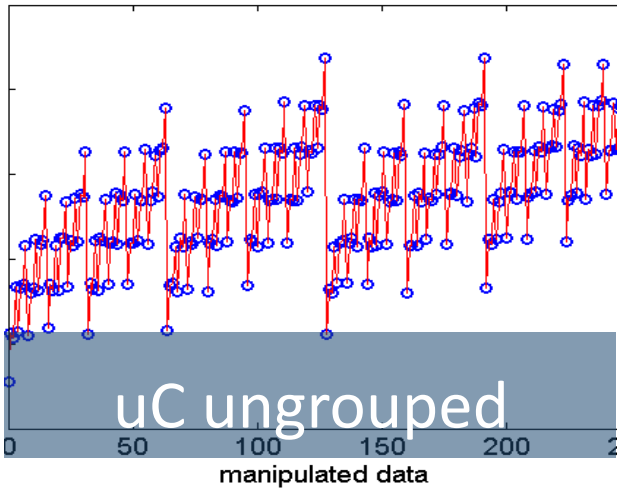
Tel Aviv University

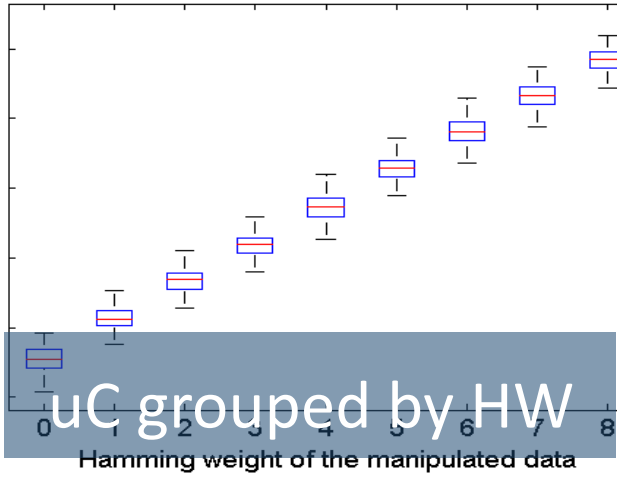
Versatility of Template-TASCA

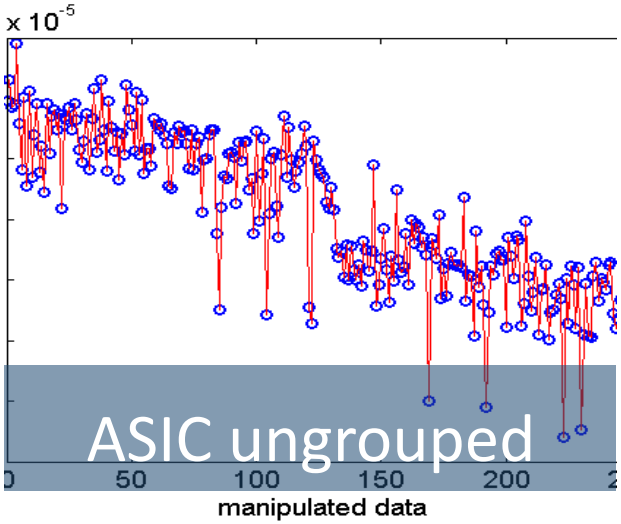


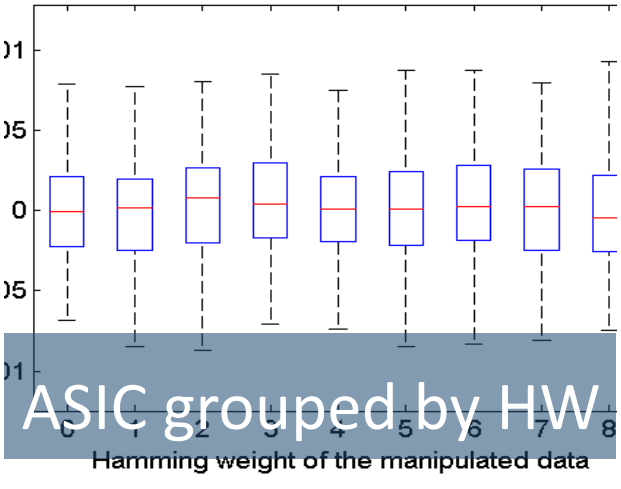
Tel Aviv University

Two cases of successful key recovery









Tel Aviv University

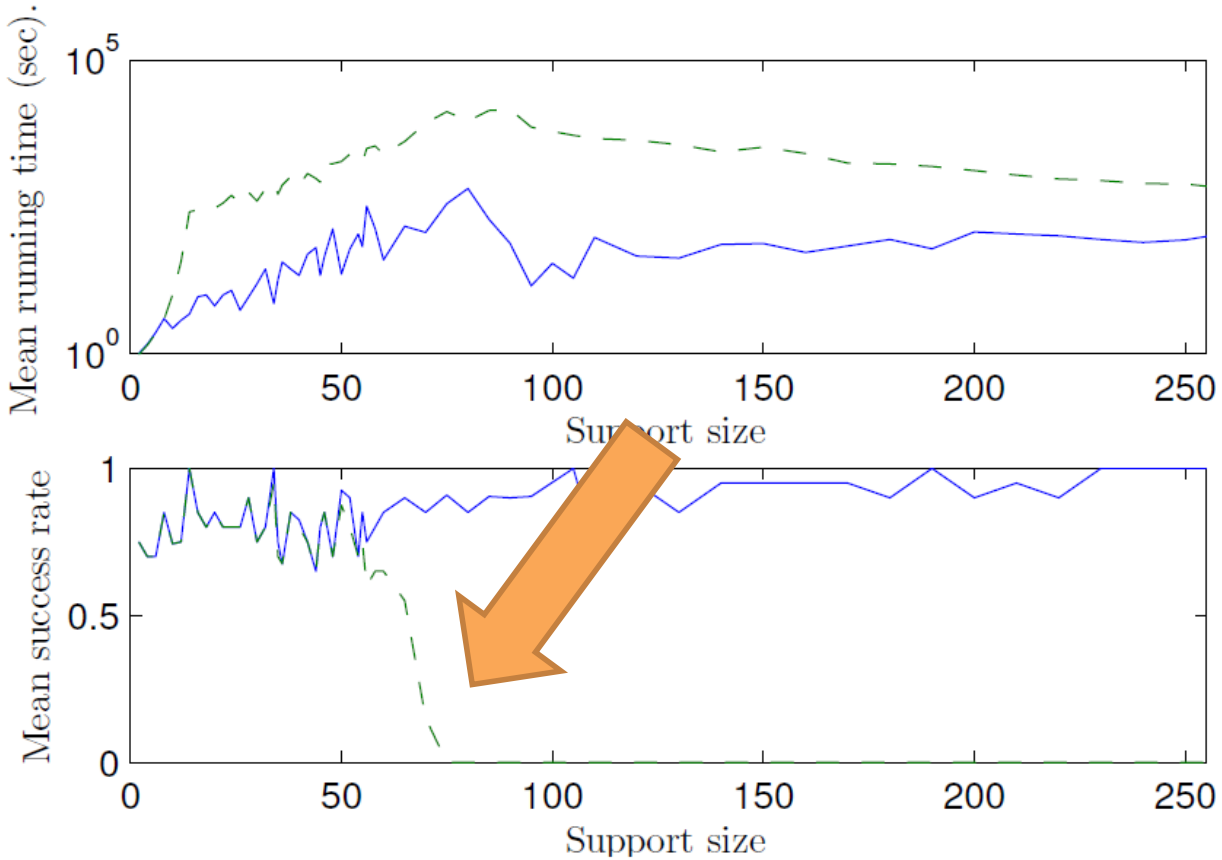
Solvers and Optimizers

- Solvers are fast, optimizers are versatile

attack	set size	decoding success	key rec. success	med. solving time	max. solving time	# of correct key bytes
set-ASCA	1	0%	0%	N/A	N/A	N/A
set-ASCA	2	83%	83%	2 seconds	6 seconds	16
set-ASCA	3	100%	0%	24+ hours	24+ hours	N/A
basic TASCA	1	0%	0%	N/A	N/A	N/A
basic TASCA	2	83%	75%	43.7 minutes	11.8 hours	14.48
basic TASCA	3	100%	80%	16.8 hours	66 hours	13.25
prob. TASCA	1	0%	0%	N/A	N/A	N/A
prob. TASCA	2	83%	82%	56.7 minutes	10.07 hours	15.88
prob. TASCA	3	100%	100%	8.2 hours	143 hours	16

Solvers and Optimizers

- Solvers cannot operate over the entire solution space (need additional heuristics)



Tel Aviv University

Shopping list

- Device under test (DUT)
- Template decoder
- Optimizer (or solver)
- Cipher equations
- Leak equations

Tel Aviv University

Start like template...

- In offline phase, create template decoders for **many intermediate states**
- In online phase, apply decoders to power trace, obtaining **multiple aposteriori probability vectors**

Tel Aviv University

… end like TASCA

- Pass probability vectors, together with device description, to **optimizer or solver**
- The output will be the state (and key) which **optimally matches** the probabilities of **all the intermediate values:**

$$x_1 \cdots x_m = \arg \max_{x_1 \cdots x_m} \prod_{i=1 \cdots m} \Pr(x_i | trace) \; s.t. \text{ cipher eq'ns are satisfied.}$$

Tel Aviv University

Summary

- Using Template-TASCA and Template-Set-ASCA, crypto devices can be attacked with **very low data complexity**
- Any leak can be used, as long as a "**soft decoder**" exists for it
- This is theoretically a very strong attack – can it have impact on real world devices?

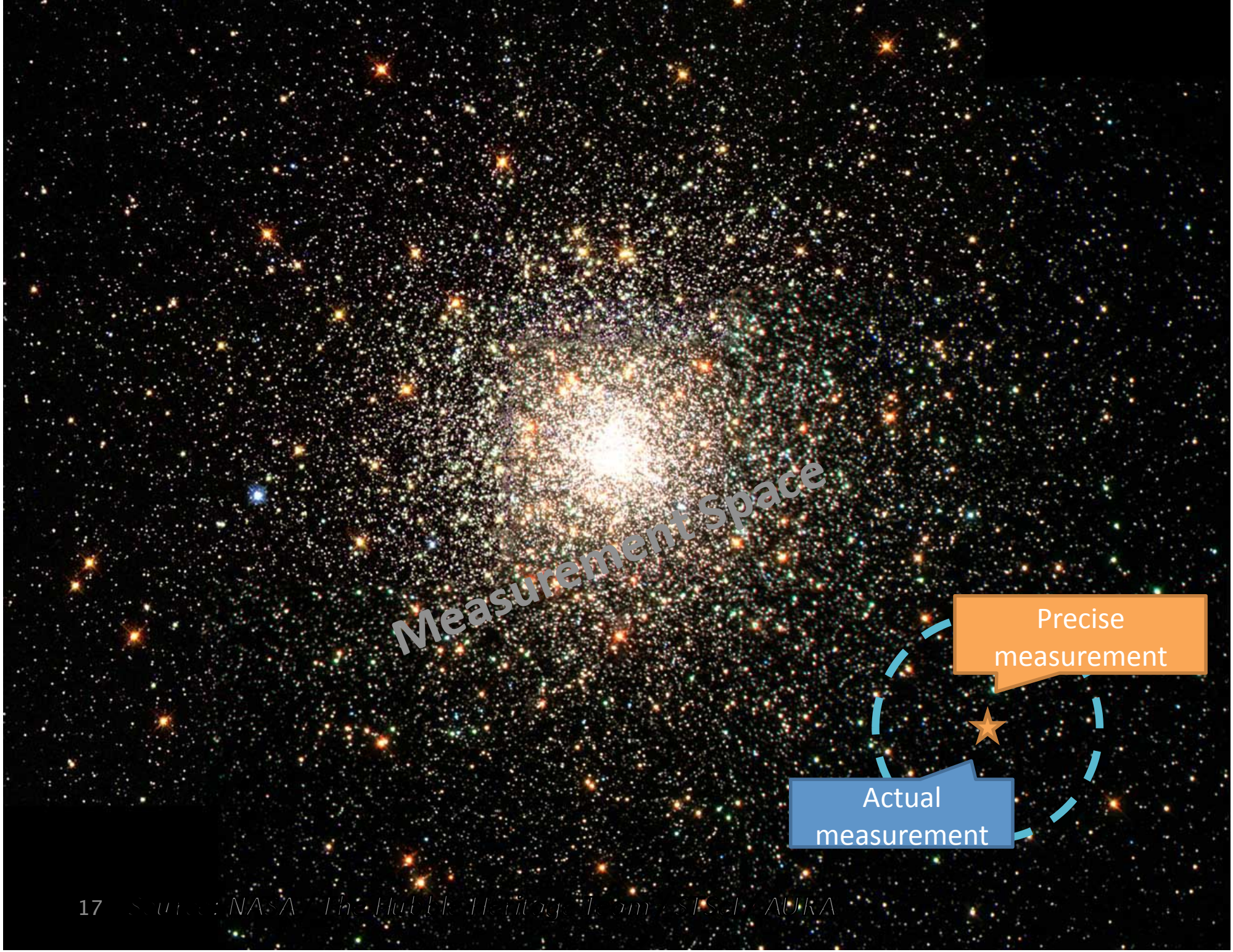
Tel Aviv University

Thank you!

http://iss.oy.ne.ro/Template-TASCA

Tel Aviv University

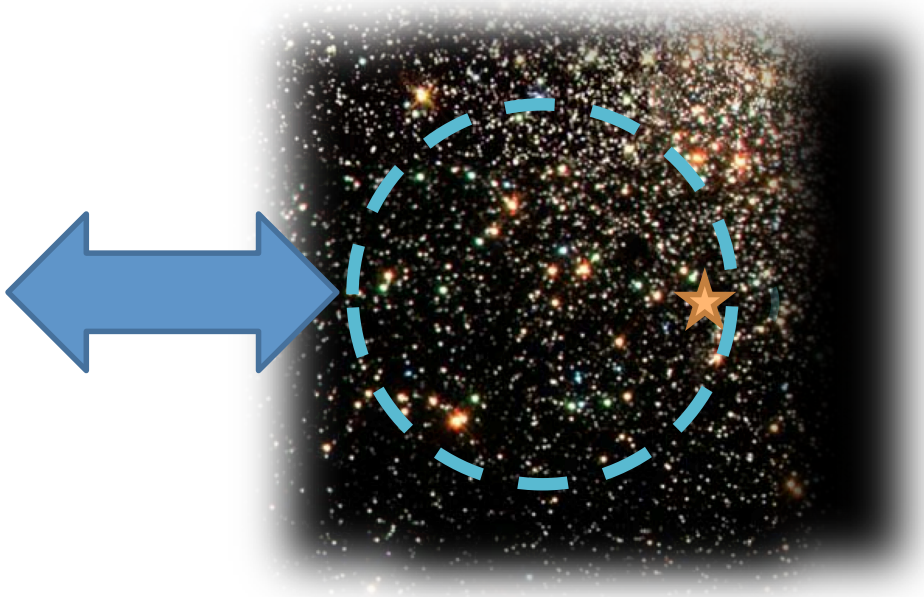
The Information-Robustness Tradeoff


Measurement Space
Precise measurement
Actual measurement

Tel Aviv University

The Harsh Reality of Power Analysis

- The side channel traces have **errors**
- Equation set with errors causes **unsatisfiability**
- Compensating for errors causes **intractability**



Tel Aviv University

Decoder does not have to be very good!

- In our experiment:
  - Ensemble of 100 decoders for intermediate bytes
  - Average rank of correct byte in decoder output: 14/256
  - Worst-case rank of correct byte: 90/256
  - Success rate: 100%