Towards Sound and Optimal Leakage Detection Procedure

A. Adam Ding[1], Liwei Zhang[1], Francois Durvaux[2], Francois-Xavier Standaert[2], and Yunsi Fei[1]

1. Northeastern University, Boston, MA, USA
2. Universite catholique de Louvain, Belgium

Northeastern University

Leakage Detection versus Identification

- Certification of crypto implementations' side-channel leakage.
- **Identify** how much (explorable) leakage exists -- stronger inference (e.g. Durvaux and Standaert 2016)
- **Detect** if any (generic) leakage exists

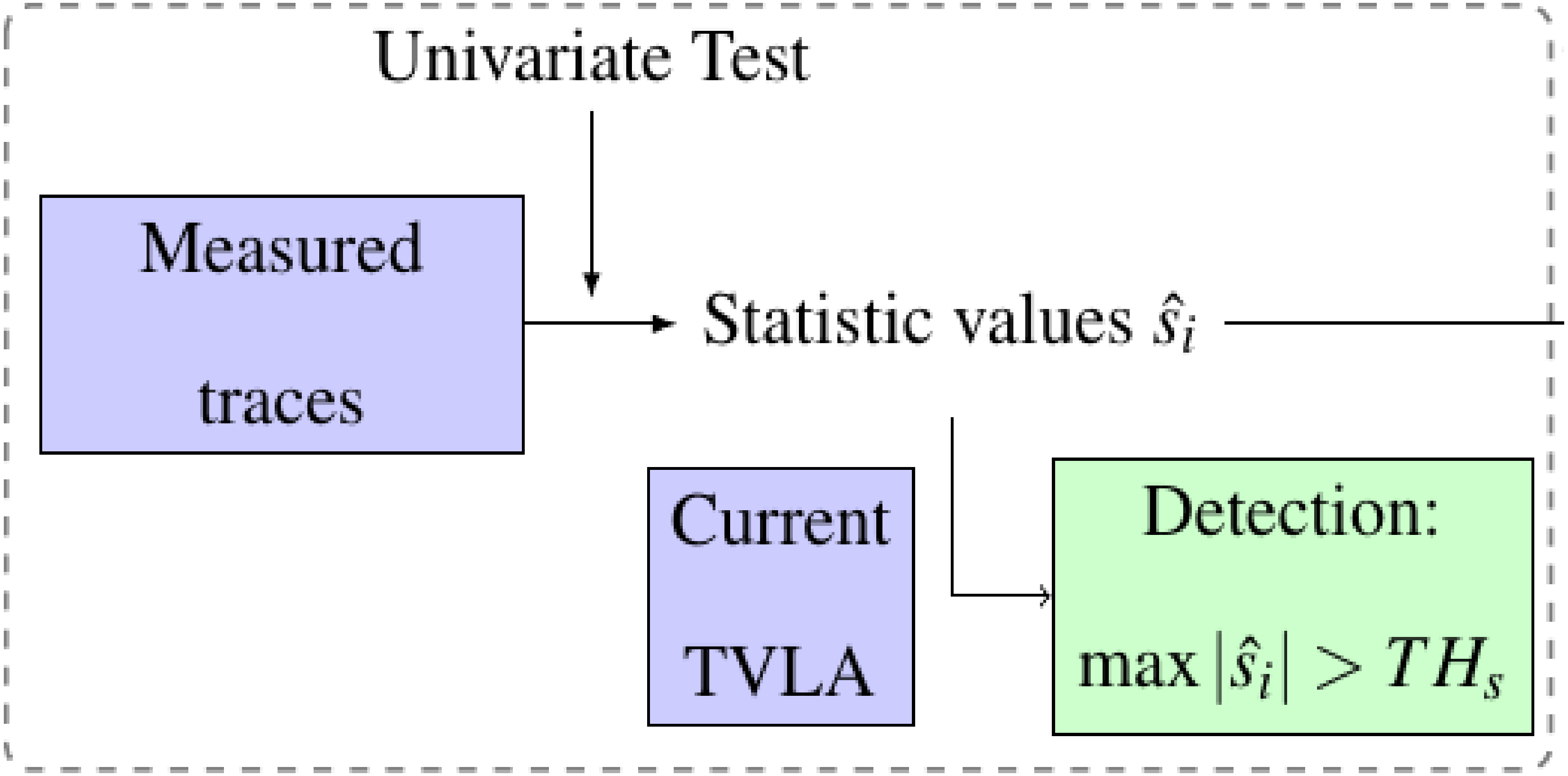
-- TVLA framework: make it sound and statistical optimal our aim here.

Test vector leakage assessment (TVLA)

- Apply a vector of univariate tests to
  - Every time point on the measurement trace
  - For leakage of intermediate variables
  - Device fails when at least one of the tests fails
- First proposed by Cryptography Research group at the 2011 NIST workshop

Abstraction of TVLA

- Scan trace of length n_L



- For t-test, leakage exists for TH=4.5

Some related work on TVLA

- T-test is the generic univariate test to use: (Mather et al. 2013)
- Higher-order/multivariate test in TVLA (Schneider and Moradi 2015 CHES)
- Question on the framework: How should we decide the overall detection (threshold) from the n_L tests on trace.
  - Balasch et al 2014: TH=5.0 for longer traces

Our proposals on TVLA

- Sound: decide the detection limit (threshold), changing with trace length n_L and sample size n_{tr}, to satisfy a fixed type I error rate α
- Statistical optimal: combine the n_L univariate tests using Higher Criticism (HC)

Issue with fixed threshold in TVLA

- T-test: Two groups A and B (fixed-vs-fixed, fixed-vs-random). Differences?

$$\widehat{s}_i = \frac{\overline{L}_{i,A} - \overline{L}_{i,B}}{\sqrt{\frac{\hat{v}^2_{i,A}}{n_A} + \frac{\hat{v}^2_{i,B}}{n_B}}},$$

- Reject null hypothesis (i.e., leakage exists) if $\max|\hat{S}_i| > 4.5$
- The type I error rate changes with n_L

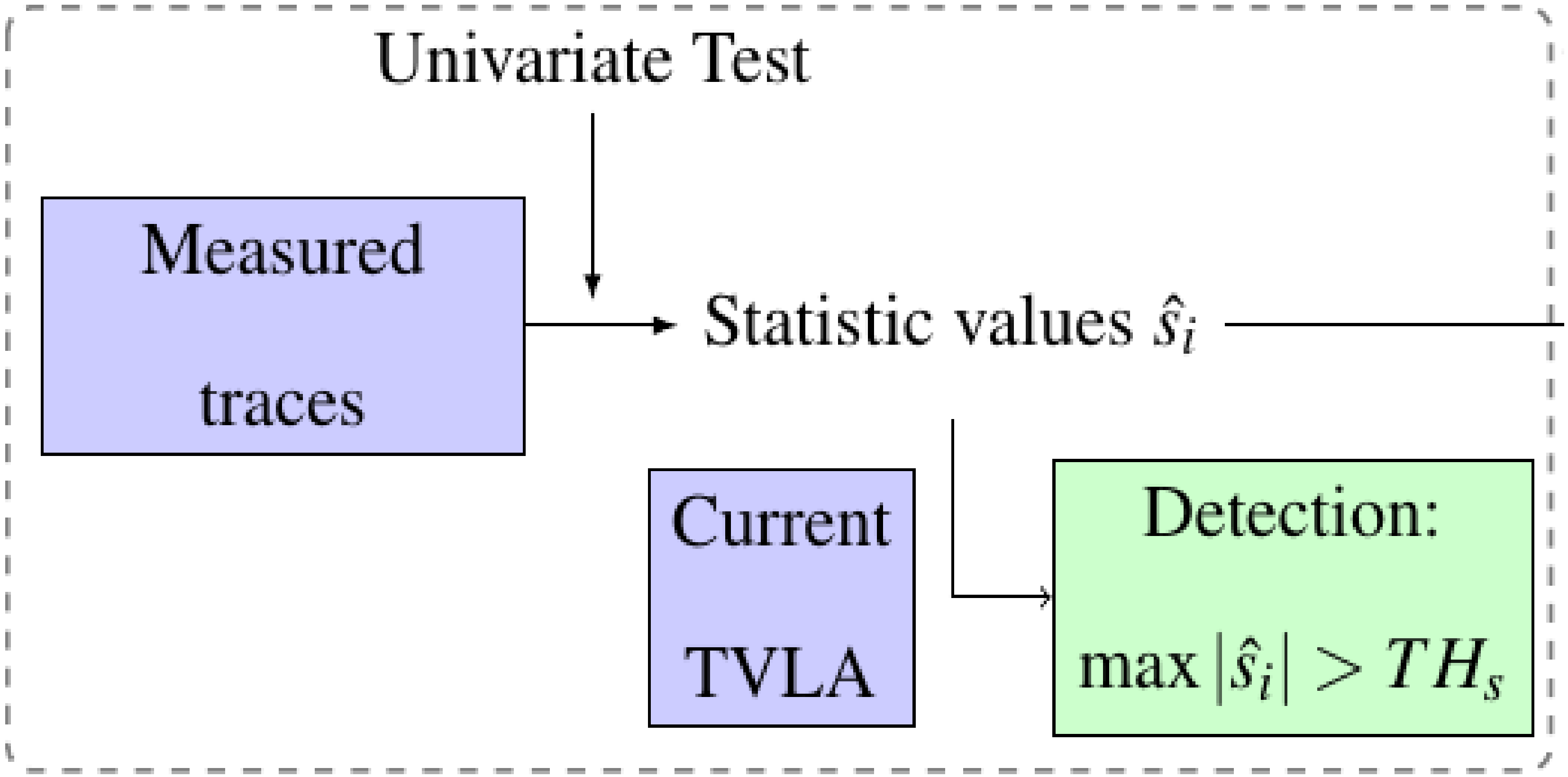
Issue with fixed threshold in TVLA

- T-test: Reject null hypothesis (i.e., leakage exists) if $\max|\hat{S}_i| > TH$
- The type I error rate changes with n_L

n_L	10^2	10^3	10^4	10^5	10^6
$\mathrm{TH} = 4.5$	0.00068	0.0068	0.0661	0.4957	0.9987
$\mathrm{TH} = 5$	0.000057	0.00057	0.0057	0.0557	0.4363

- A safe device will fail if n_L=1million

TVLA threshold through p-values



- This is mini-p procedure: $\min|p_i|$<TH_p
- $TH_p = 1 - (1-\alpha)^{1/n_L}$

TVLA threshold through p-values

- T-test:

$$\widehat{s}_i = \frac{\overline{L}_{i,A} - \overline{L}_{i,B}}{\sqrt{\frac{\hat{\nu}^2_{i,A}}{n_A} + \frac{\hat{\nu}^2_{i,B}}{n_B}}}, \quad p_i = 2 \times \left(1 - \mathrm{CDF}_t(\widehat{s}_i, \hat{\nu}_i)\right),$$

- CPA (ρ-test) $\hat{\rho}_i = \mathrm{Corr}(L_i, V).$

$$\widehat{s}_i = \frac{1}{2} \ln\left(\frac{1+\hat{\rho}_i}{1-\hat{\rho}_i}\right)\sqrt{n_{tr}}. \quad p_i = 2 \times \left(1 - \mathrm{CDF}_{N(0,1)}(|\widehat{s}_i|)\right)$$

- Can work with p-values no matter what univariate test is used.

Sound mini-p threshold for t-test in TVLA

(b) Threshold values TH under fixed type I error rates.

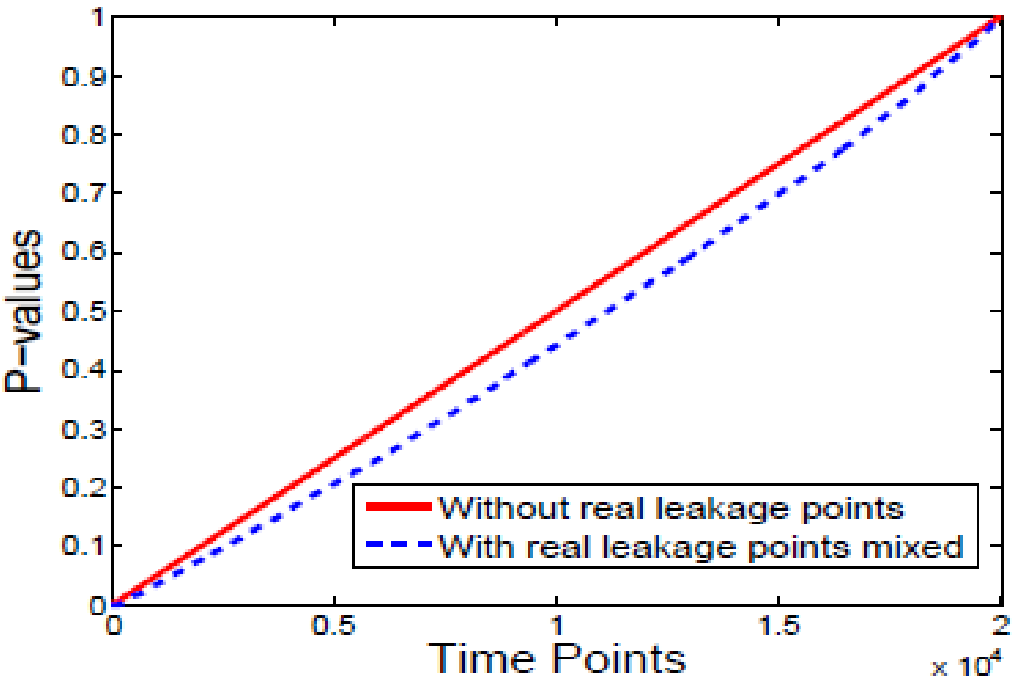
n_L	10^2	10^3	10^4	10^5	10^6	10^7	10^8
$\alpha = 0.001$	4.417	4.892	5.327	5.731	6.110	6.467	6.806
$\alpha = 0.01$	3.889	4.416	4.891	5.326	5.730	6.109	6.466

- Choose an α value, then find the threshold for mini-p procedure.

Using Higher Criticism in TVLA

- Mini-p is not statistical optimal, replace with Higher Criticism (HC): compare the p-values to uniform distribution.

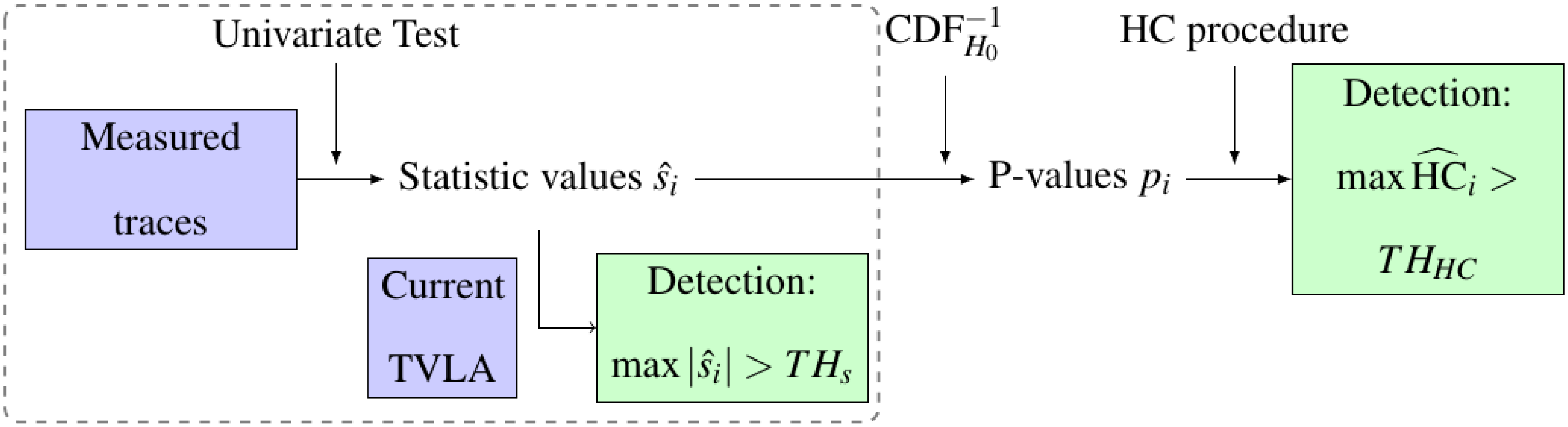
$$\hat{p}_{(1)} \leq \hat{p}_{(2)} \leq \cdots \leq \hat{p}_{(n_L)}$$



$$\widehat{HC}_{n_L,i} = \frac{\sqrt{n_L}\left(i/n_L - \hat{p}_{(i)}\right)}{\sqrt{\hat{p}_{(i)}\left(1-\hat{p}_{(i)}\right)}}$$

Leakage Detection Procedure: HC

- distance $$\widehat{\mathrm{HC}}_{n_L,i} = \frac{\sqrt{n_L}(i/n_L - \hat{p}_{(i)})}{\sqrt{\hat{p}_{(i)}(1-\hat{p}_{(i)})}}, \quad i = 1, \ldots n_L$$



- HC leakage detection procedure is optimal in high-dimensional setting (long trace here).

Optimality of HC Leakage Detection

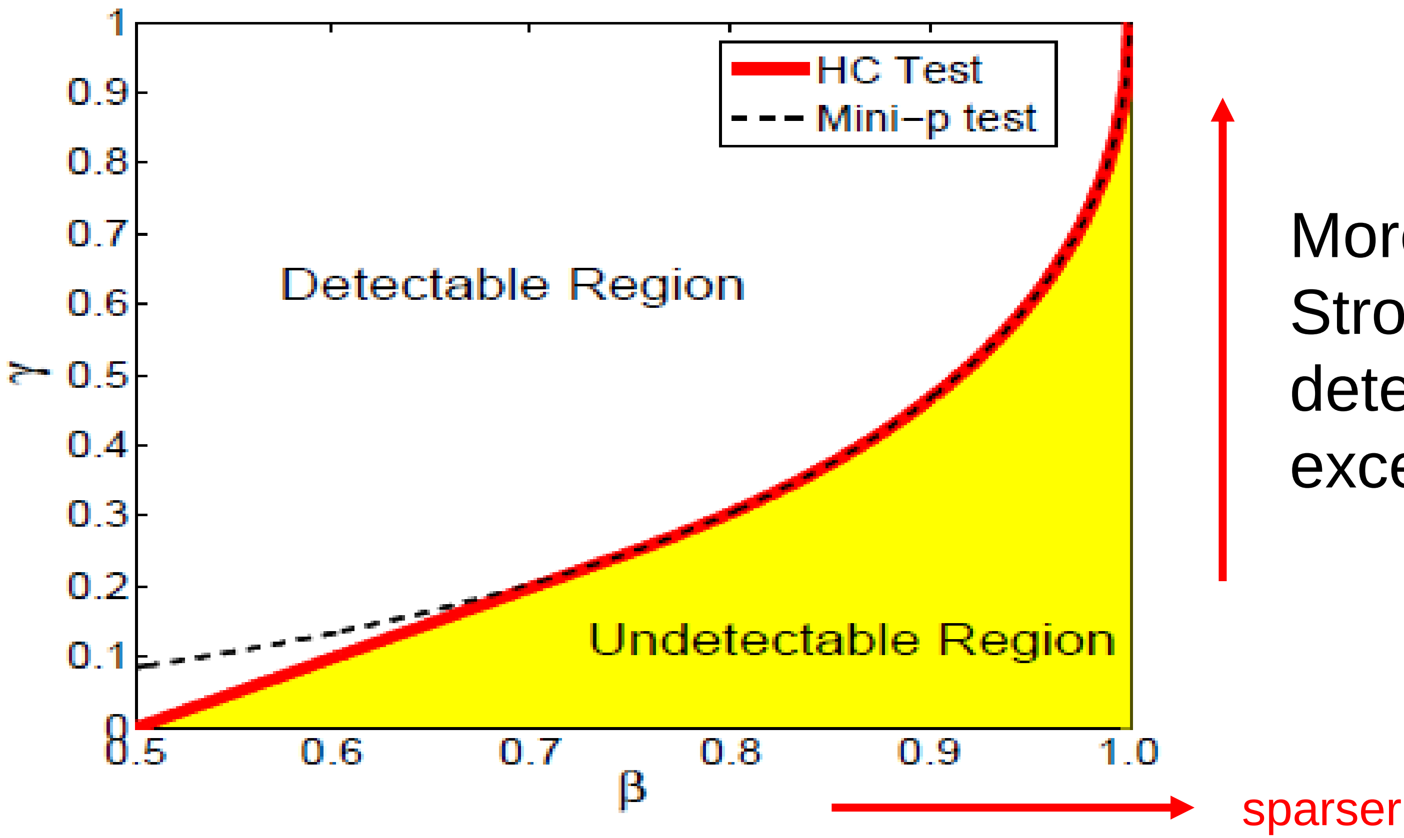
- Model $L_i = \tilde{V}\delta_i + r_i, \quad i = 1, \cdots, n_L$
- Model SNR $= Var(V\delta_i)/Var(r_i) = \delta_i^2$
- Test statistic $\hat{S}_i$ → $N(\sqrt{n_{tr}\delta_{s_i}^2}, 1)$
- Test SNR $n_{tr}\delta_{s_i}^2$ with

  $\delta_{s_i}^2$ equal to or smaller than δ_i^2

- HC optimal combination given test SNR
- (optimal test for Gaussian mixture)

HC versus mini-p (better when multiple signals)

- Given q proportion each SNR Δ^2.
- Sparsity $\beta = -\log(q)$,signal $\gamma = \Delta^2/2\log(n_L)$



More traces n_{tr} Stronger signal, detection when exceed

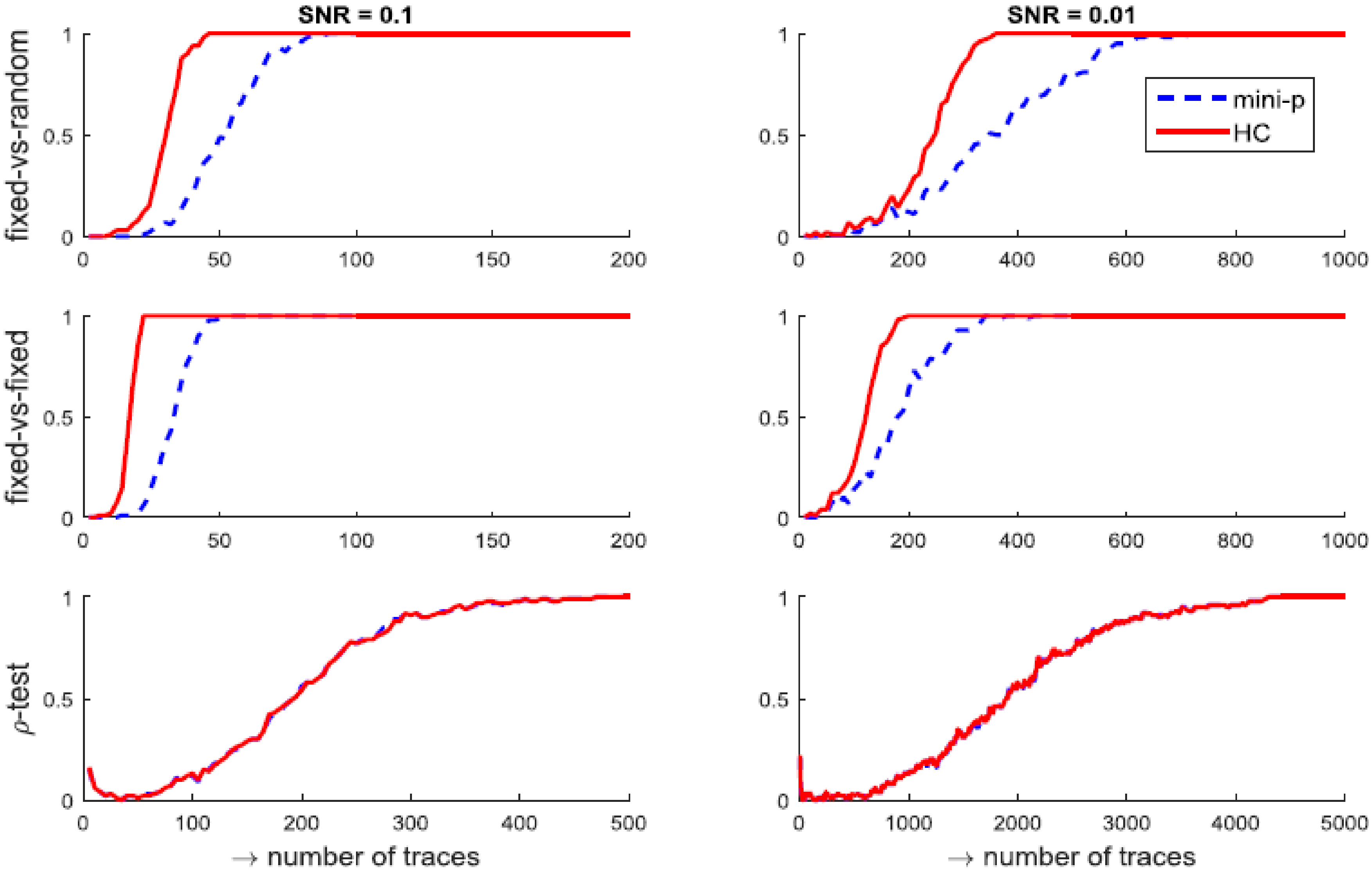
Numerical Examples

- Simulation of 8-bit AES-128 Hamming Weight leakage with Gaussian noise. n_L=496
- Implementation of unprotected AES on a SASEBO-W board. n_L=50,000.
- Implementation of masked AES on a SASEBO-GII board. Detection of 2nd-order (bivariate) centered-product leakage. n_w=3125, $n_L=(n_w^2+n_w)/2$

Numerical Examples: Simulation

- (i) t-test with fixed-vs-random plaintexts
- (ii) t-test with fixed-vs-fixed plaintexts
- (iii) ρ-test with random plaintexts
- (i) and (ii) non-specific tests, non-sparse signals. HC versus mini-p: higher detection power.
- (iii) specific test, sparse signal. HC versus mini-p: same.

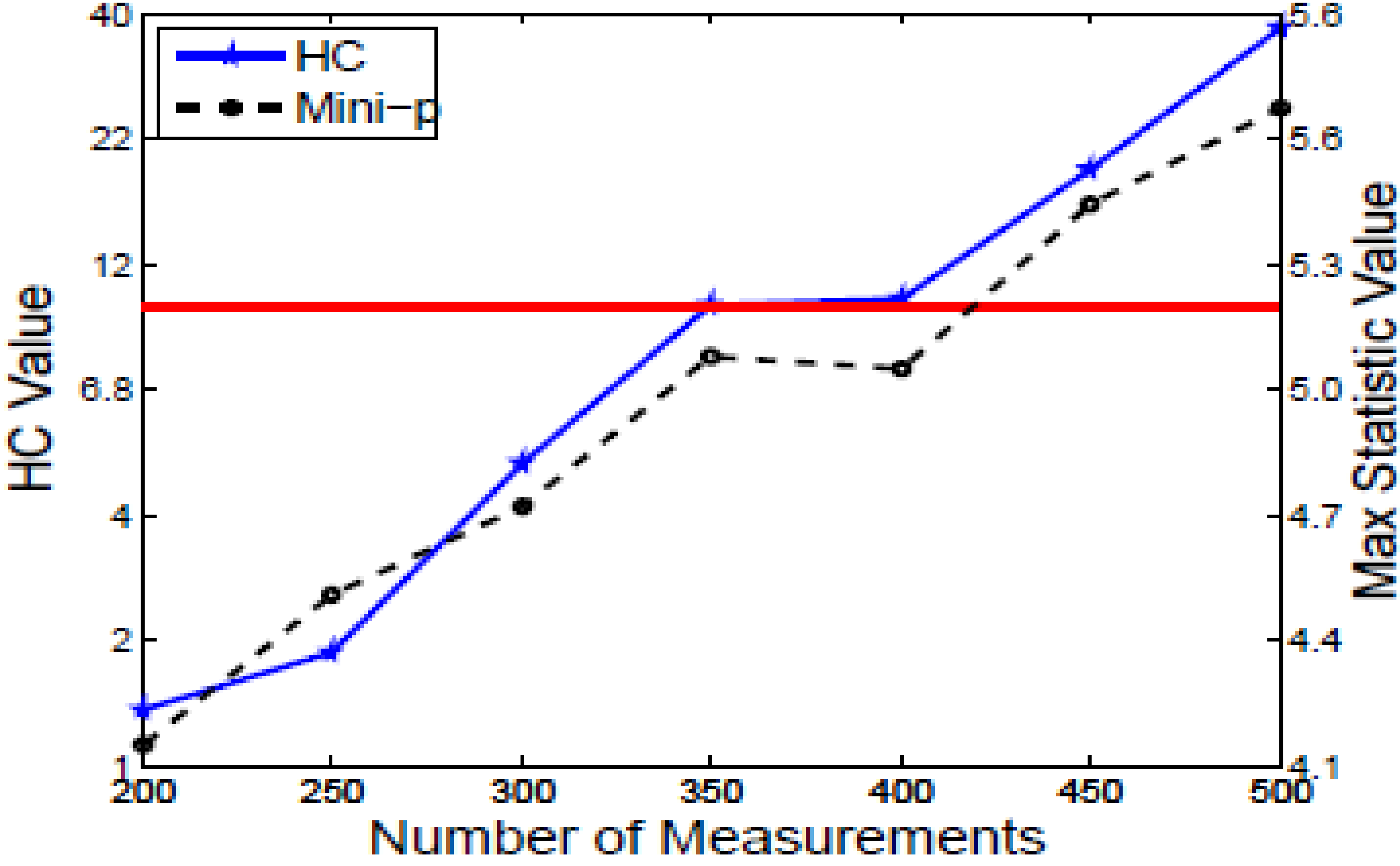
Numerical Examples: Simulation



Numerical Examples: Real implementations

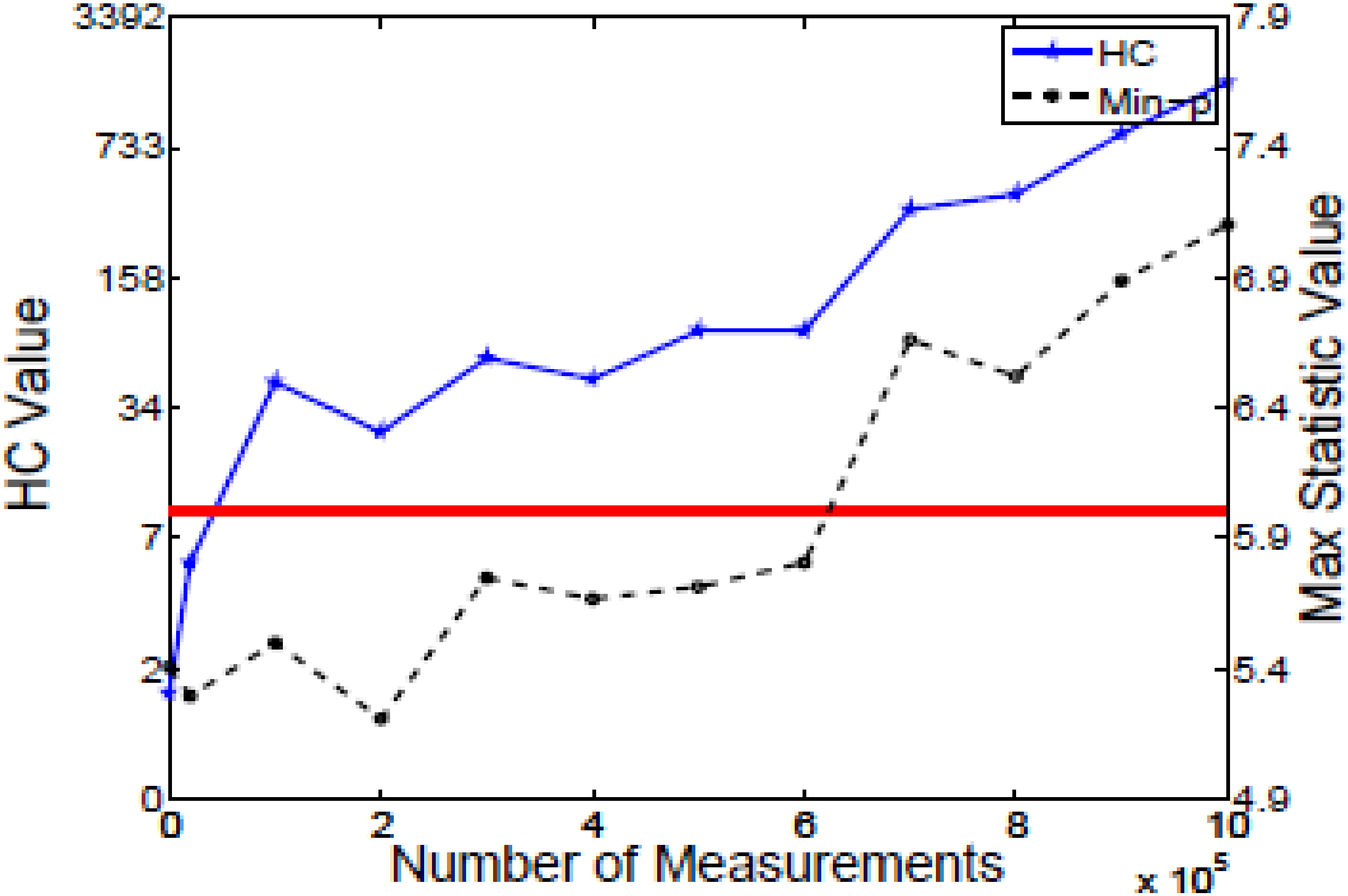
- ρ-test with random plaintexts
- Unprotected AES: HC a bit better than mini-p. (Signals sparse and strong)
- Masked AES: HC much better than mini-p. (Multiple signals)

Numerical Examples: Unprotected AES



(a) Unprotected AES data

Numerical Examples: Masked AES (2^{nd}-order)



Discussion

- Usage: leakage detection
  - Pass if the optimal HC procedure does not detect any for the specified number of traces.
  - If detected, explorable leakage? (identify/quantify, may need more traces.)
- Issue and future work:
  - Assumption of independence across different time points on the trace.
  - Use generalized HC (JASA2017) to deal with dependence.

Summary

- Improve the TVLA framework
- Sound detection limit by Type I error rate
- HC procedure (statistical optimal) has better detection power.

Question?

- Acknowledgments: NSF funding: CNS-1314655,CNS-1337854, CNS-1563697; European Commission funding: H2020 project 731591 and the ERC project 724725.