Clustering Algorithms for Non-Profiled Single-Execution Attacks on Exponentiations

Johann Heyszl[1] Andreas Ibing[2] Stefan Mangard[3,4]
Fabrizio De Santis[2,4] Georg Sigl[2]

[1]Fraunhofer Research Institution AISEC, Munich, Germany
[2]Technische Universität München, Munich, Germany
[3]Graz University of Technology, Graz, Austria
[4]Infineon Technologies AG, Munich, Germany

Motivation

- Single execution side-channel attacks on exponentiations
- Previous ones require profiling or manual tuning or use ad-hoc algorithms
- We describe how to use cluster classification algorithms instead

Reminder: Exponentiation Algorithms

- Exponentiations in asymm. crypto
  - Modular exponentiations in RSA
  - Elliptic curve scalar multiplications in ECC
- Popular algorithms:
  - Square-and-multiply-always (RSA) / double-and-add-always (ECC)
  - Montgomery ladder (RSA, ECC)
- Key features of exponentiation algorithms
  - Secret exponent processed bit/digit-wise in loop
  - Mostly timing-safe, hence, operation sequence uniform (against SPA)

Single-Execution Leakage

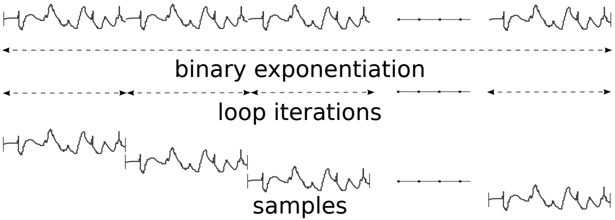
- Side-Channel Attackers only have **single observations** to exploit
  - Due to ephemeral exponent or e.g. blinding countermeasure

Single-Execution Leakage

- Side-Channel Attackers only have **single observations** to exploit
  - Due to ephemeral exponent or e.g. blinding countermeasure

- **Certain amount of information about exponent bits** (binary alg.) is still leaking in most cases $\rightarrow$ **single-execution leakage** (adress-bit-related, localized leakage, ...

Exploiting Single-Execution Leakage



- Cut recorded exponentiation trace into samples
- Each corresponds to different secret bit (binary exp. alg.)
- **Attack basically means to find correct partition = Classification**

Exploiting Single-Execution Leakage
Previously and Strongly Related

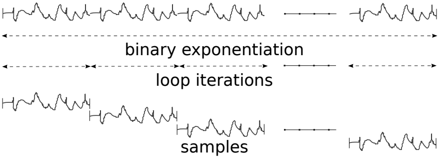
- **Template attacks**
  - **Require profiling** (difficult, think of e.g. blinding)
- **Cross-correlation-based attacks**
  - Requires **manually tuned thresholds**
  - Correlation disregards information (absolute values)
  - Some are based on heuristic power models
    (corr. coeff. makes more sense then)
- **Walter's Big Mac attack** from 2001
  - Ad hoc engineered algorithm

Our Proposal
Using Unsupervised Clustering for an Attack

- Use algorithms from the established research-field of '**Pattern classification**'
  - Those are already heavily researched in other applications
- We propose to use **unsupervised cluster classification algorithms**
  - Exploit single execution leakage of exponentiation algorithms

Our Proposal
Using Unsupervised Clustering for an Attack

- Reminder: In *profiled template attack*, cut-out samples are *classified* by *matching to templates*



- Clustering algorithms **classify** the cut-out samples **automatically without profiling or manual tuning**
  - Unknown if **0** or **1** bits, but easy try-out

- Success depends on available leakage of course

Unsupervised Cluster Classification Algorithms

- Unsupervised means no training data, no profiling
- Input a set of multi-dimensional samples/vectors e.g. cut-out trace-parts
- Algorithm estimates distributions
- Define free parameters of distribution (e.g. *two* cluster centers)
- Optimal algorithm depends on the distribution model (shape of clusters)

Unsupervised Cluster Classification Algorithms
K-Means

- Example algorithm:
  ***k*-means** algorithm for **unsupervised clustering**
  - Finds ***k*** cluster centers and corresponding classification
  - Distribution assumption - shape of clusters:
    - *k* equal Gaussian distributions
    - Independent values in samples (dimensions are independent)
    - Variance equal within clusters

Unsupervised Cluster Classification Algorithms
K-Means

- **Input:** Samples (cut-out trace parts) and number of clusters k
- Starts by choosing k **random** samples as initial cluster means
- Then iteratively:
  - Compute *Euclidean distance* from all samples to current k means
  - Classification: *Assign all samples to closest mean* $\rightarrow$ k classes
  - **Compute new means** of k classes from current classification
  - Repeat *until no change in class assignment*
- **Output:** k cluster means and classification
- Repeat with different starting points to prevent local maxima (best outcome based on sum-of-squared-error criterion selected)

Fraunhofer AISEC

Practical Evaluation

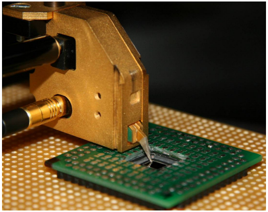
- Laboratory setup (FPGA-based , trigger output, synchronized clock) (Definitely not real world ;)
- Same setup as in our CT-RSA'12 paper:
  Template attacks exploiting location-based leakage

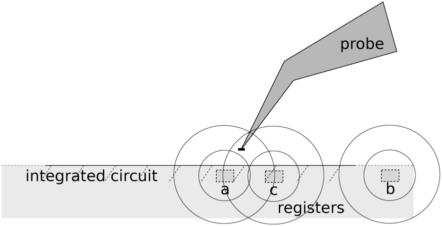
Practical Evaluation
FPGA DUT

- Straight-forward FPGA-based digital HW implementation:
  - Elliptic curve scalar multiplication ($Q = d \cdot P$) with affine input/output
  - López and Dahab Montgomery ladder 'exponentiation' algorithm, binary field $GF(2^{163})$, NIST parameters

Practical Evaluation
Location-Based Leakage

- High-resolution inductive near-field probe (**100 μm** resolution)
- Probe is closer to one of two registers
- Register access depends on current secret bit in loop

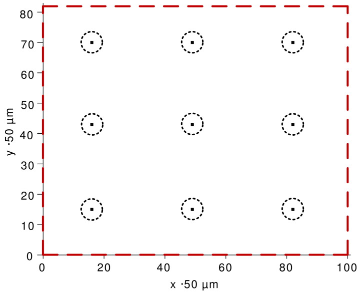




Fraunhofer AISEC

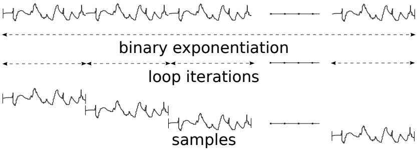
Practical Evaluation
Measurement Positions

- FPGA die surface
- Multiple measurement positions in geometric regular array (no profiling to find locations)



Practical Evaluation
Trace Example

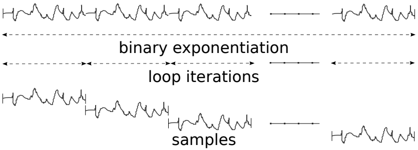
- Reminder: Cutting a trace into samples



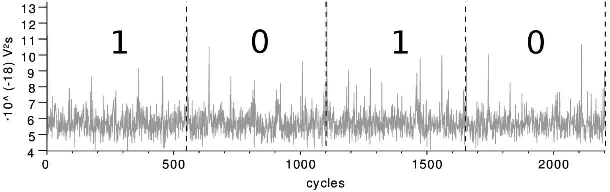
Fraunhofer AISEC

Practical Evaluation
Trace Example

- Reminder: Cutting a trace into samples



- Example from one measurement - 4 samples



Fraunhofer AISEC

Practical Evaluation
Result from One Position

- Single measurement **after** clustering
  - Returns 2 sample means and corresp. classification

Practical Evaluation

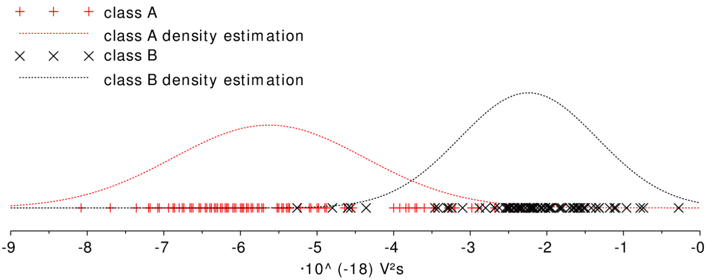
Result from One Position

- Single measurement **after** clustering
  - Returns 2 sample means and corresp. classification
  - **For visualization:**
    - Regard the samples/means as vectors in multi-dim. space
    - Draw line through to means
    - 1-D projection of samples on this line

Fraunhofer
AISEC

Practical Evaluation
Result from One Position

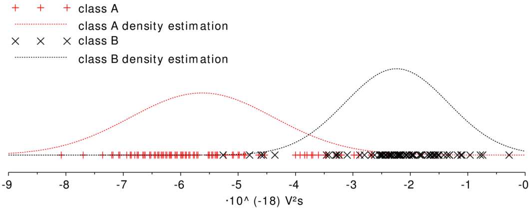
- Single measurement **after** clustering
  - Returns 2 sample means and corresp. classification
  - **For visualization:**
    - Regard the samples/means as vectors in multi-dim. space
    - Draw line through to means
    - 1-D projection of samples on this line



Fraunhofer AISEC

Practical Evaluation
How to Cope with Errors?

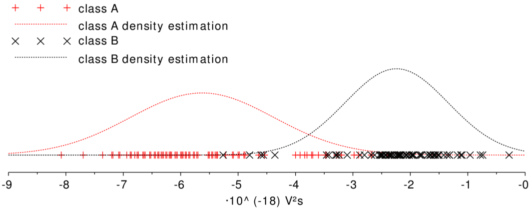
- Clustering algorithms allow to derive posterior probabilities for each sample describing likelihood of correct classification (basically low if close to separation plane)



Fraunhofer AISEC

Practical Evaluation
How to Cope with Errors?

- Clustering algorithms allow to derive posterior probabilities for each sample describing likelihood of correct classification (basically low if close to separation plane)



- Attacker may use this in a brute-force strategy:
  - Trial bits with low post. probabilities first
  - Repeat and increase number of trialed bits until correct exponent found

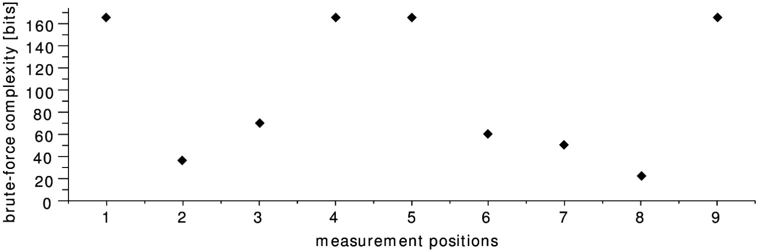
Fraunhofer AISEC

Practical Evaluation
Results for All Positions

- Estimate remaining brute-force complexity **after** clustering attack

Practical Evaluation
Results for All Positions

- Estimate remaining brute-force complexity **after** clustering attack
- All individual measurement positions:



- In **2 out of 9** cases, brute-force complexity is clearly feasible for attackers (only 2^{22} and 2^{37} trials)

Fraunhofer AISEC

Practical Evaluation
Combining Simultaneous Measurements

- What if exploited leakage is insufficient?
- Repeating measurements is impossible because exponent changes

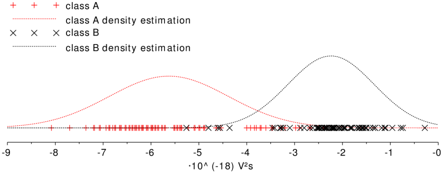
- Cluster analysis provides straight-forward possibility to combine (simultaneous) measurements:
  - Simply concatenate cut-out samples

Practical Evaluation
Improvement Through Combination

- Due to lack of mult. probes, meas. are repeated with const. inputs

Practical Evaluation
Improvement Through Combination

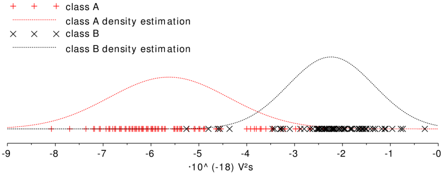
- Due to lack of mult. probes, meas. are repeated with const. inputs
- **One** measurement (**after** clustering, 1-D projection): **Many Errors**



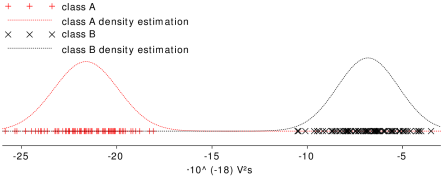
Practical Evaluation

Improvement Through Combination

- Due to lack of mult. probes, meas. are repeated with const. inputs
- **One** measurement (**after** clustering, 1-D projection): **Many Errors**



- **All** measurements (**after** clustering, 1-D projection): **No Errors**



Fraunhofer AISEC

Countermeasures

- Exponent blinding or coordinate randomization do not help
- Reduce SNR of single-execution leakage as far as possible
- Address sources of specific single-execution leakage.
  E.g. Reduce location-based leakage using interleaved placement

Fraunhofer AISEC

Conclusion

- **Non-profiled attack** against exponentiations
  - Well established clustering algorithms
  - No manual tuning
  - Can be generalized to any single-/multi-variate single execution leakage of exponentiation algorithms
  - Combination of measurements can improve attack
    $\rightarrow$ no need to find best positions

- In our opinion, this should make cross correlation-based single-execution attacks obsolete
- Clustering may also be interesting e.g. for SCA collision attacks

Thank You

Back-Up
K-Means

- Example: Graphical representation of 2-dimensional samples (not my data)
  - In this example: samples cluster around two means/centroids
  - This corresponds to binary exponentiation case
  - The segmentation can be found through unsupervised algorithms

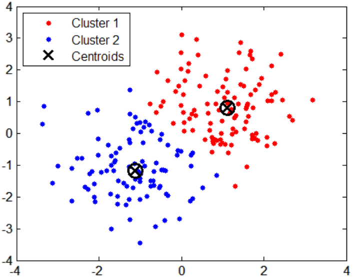


Figure: Source: `http://www.mathworks.de/de/help/stats/kmeans.html`

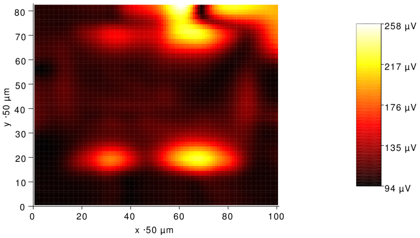
Back-Up
ECC Implementation

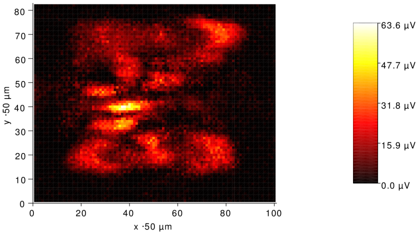
- Elliptic curve scalar multiplication ($Q = d \cdot P$)
- Binary field $GF(2^{163})$, NIST *Curve B-163* parameters
- López and Dahab Montgomery ladder 'exponentiation' algorithm
- Affine x- and y-coordinates as input and output

- Fulfills requirements for successfull attack
  - Bitwise processing of **163** bit scalar
  - Uniform operation sequence for each bit
  - Register usage **depends** on bits

Back-Up

Locations with High Leakage vs. High Amplitudes





Fraunhofer AISEC