Semi-supervised template attack

Liran Lerman, Stephane Fernandes Medeiros, **Nikita Veshchikov**,
Cédric Meuter, Gianluca Bontempi and Olivier Markowitch

Université Libre de Bruxelles, Belgium

COSADE 2013

Motivation

- Template Attack is one of the most powerful attacks
- Need to control the attacked device

Outline

- Step-by-step HOWTO
- Simulations, Experiments & Discussion
- Conclusion & Future works

HOWTO : SSTA

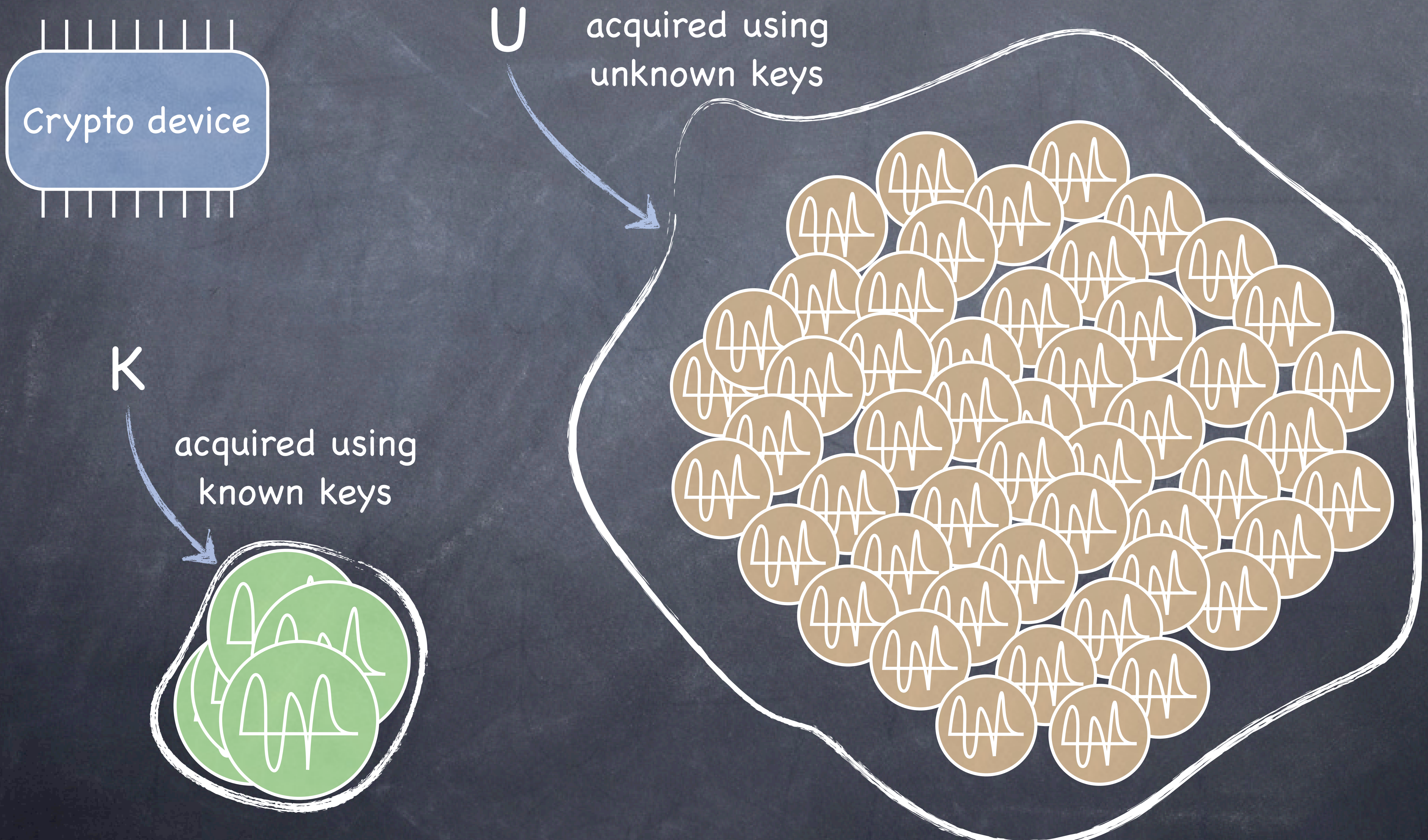
The case

- AES, 10 rounds, 128-bit key
- manipulates 1 byte at a time

Attacker

- Can collect power traces
- Has his own key
- Has several accomplices

Traces



Crypto device

U

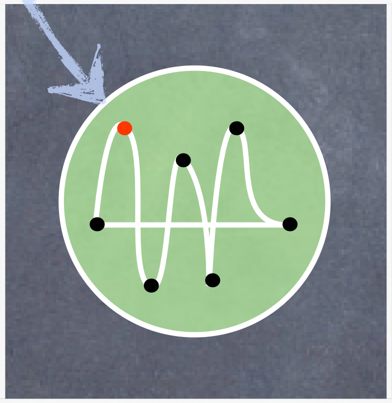
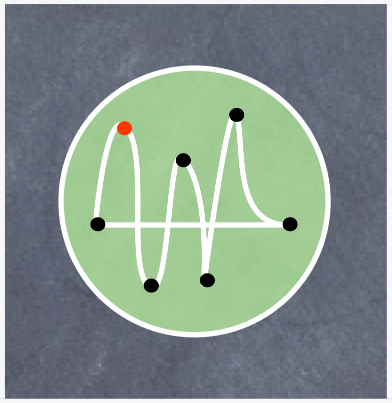
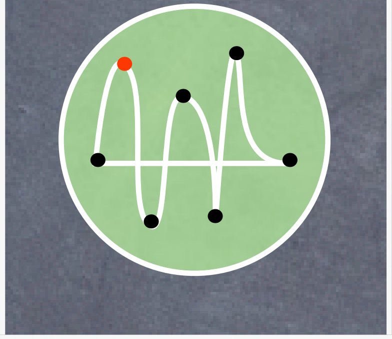
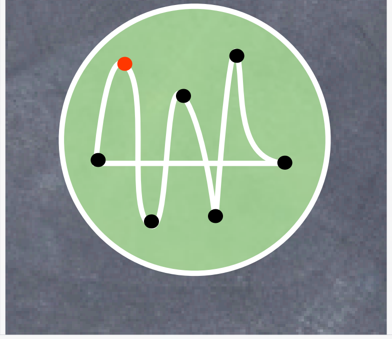
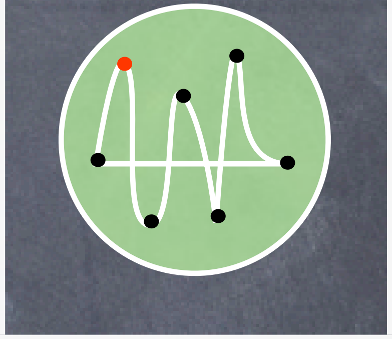
acquired using unknown keys

K

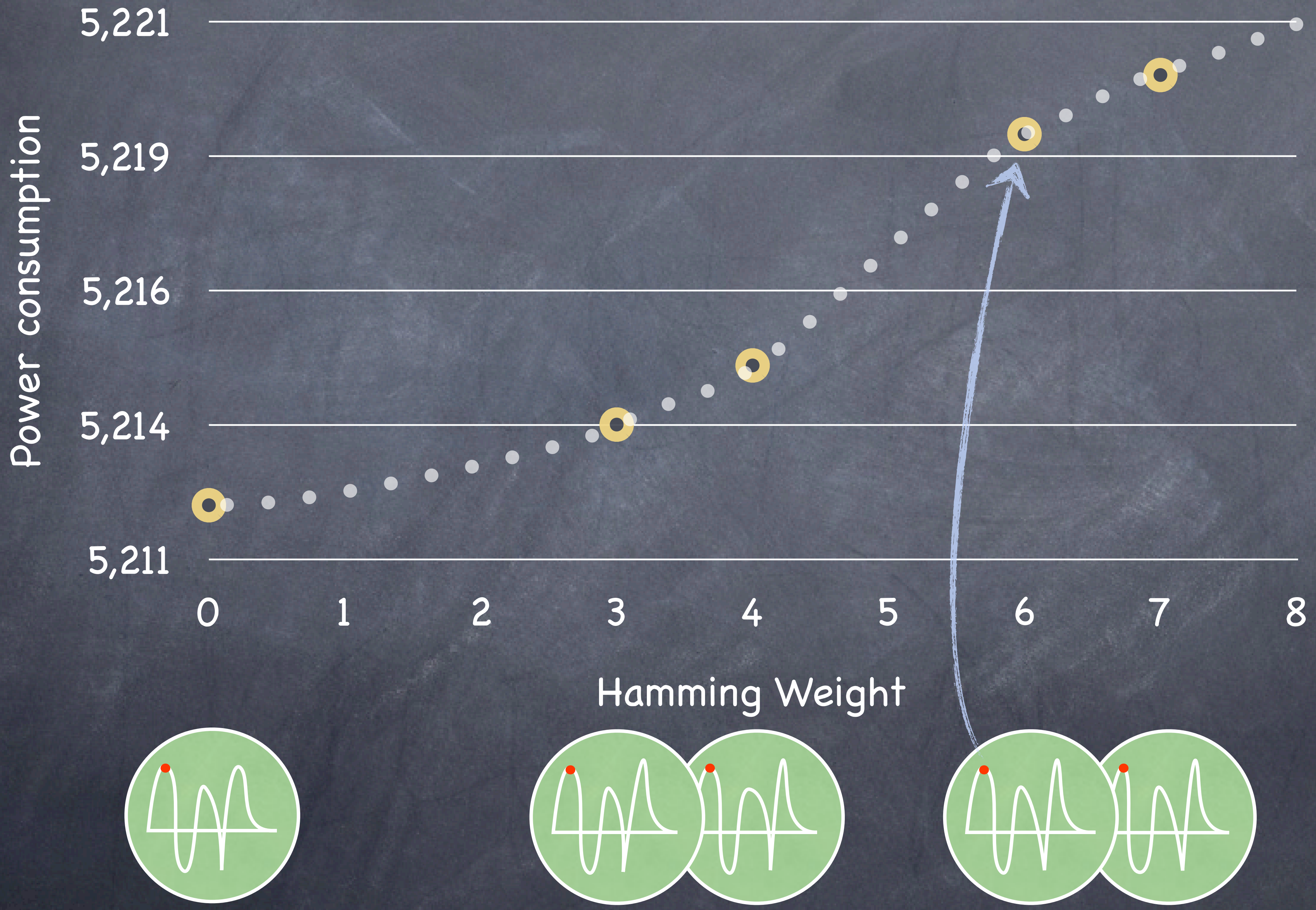
acquired using known keys

Choosing the point

Use dependency (e.g. Mutual information, Pearson correlation, ...)

					
Byte value	0x00	0x34	0x3A	0xBD	0x7F
HW	0	3	4	6	7

Power consumption



Clustering

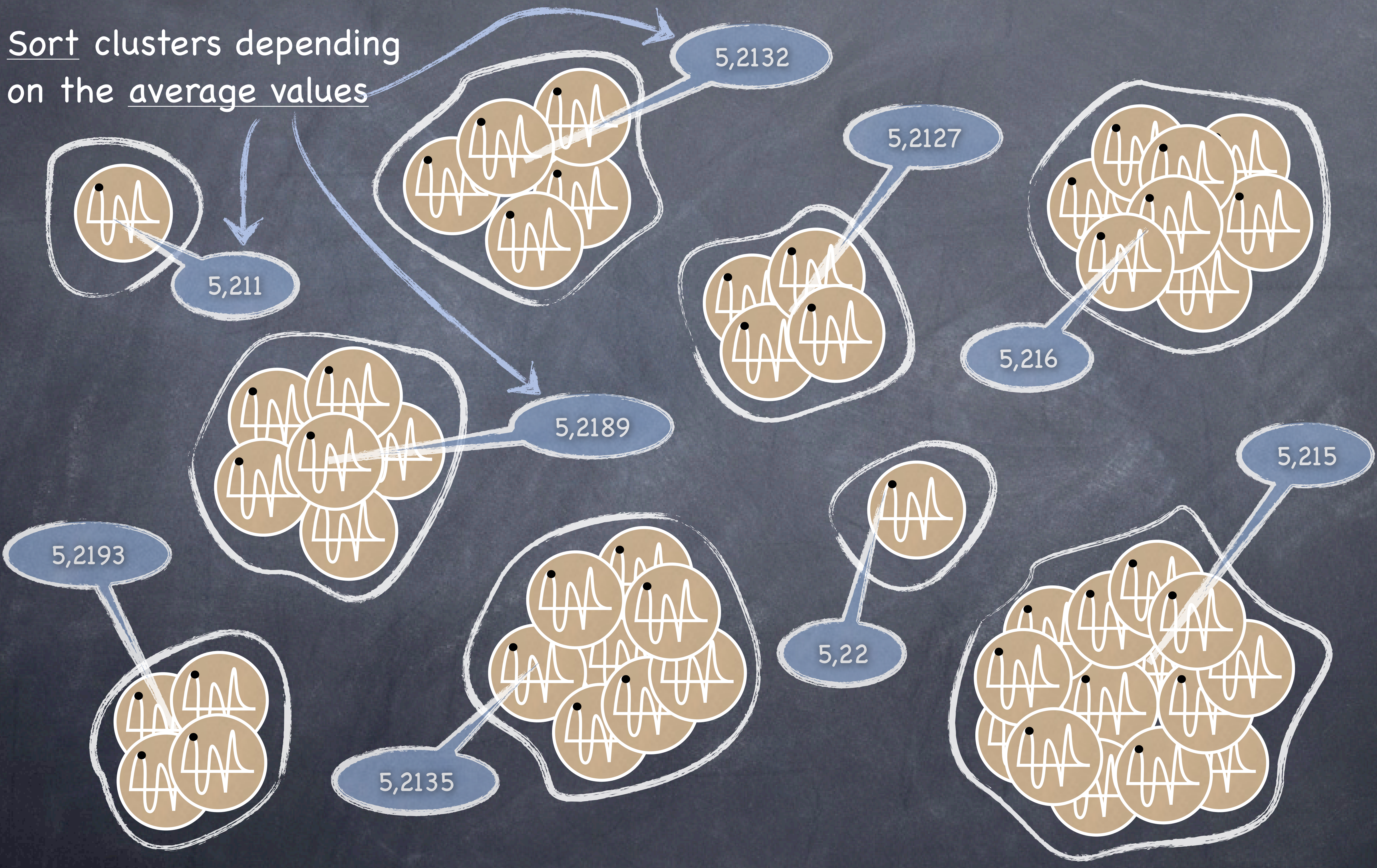
Algorithm : Clustering around medoids

Input : points and number of clusters

Clustering

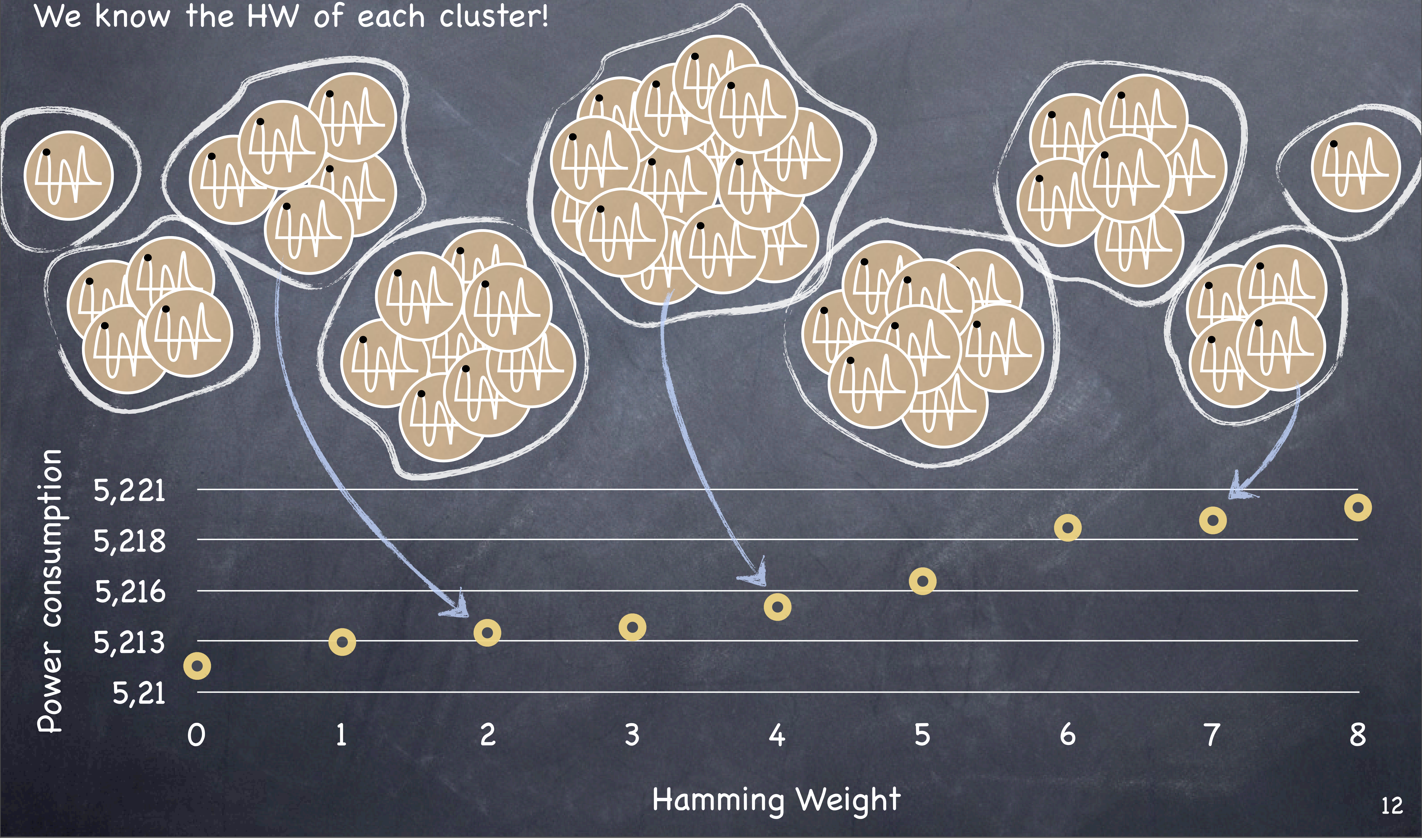
Labeling clusters

Sort clusters depending on the average values

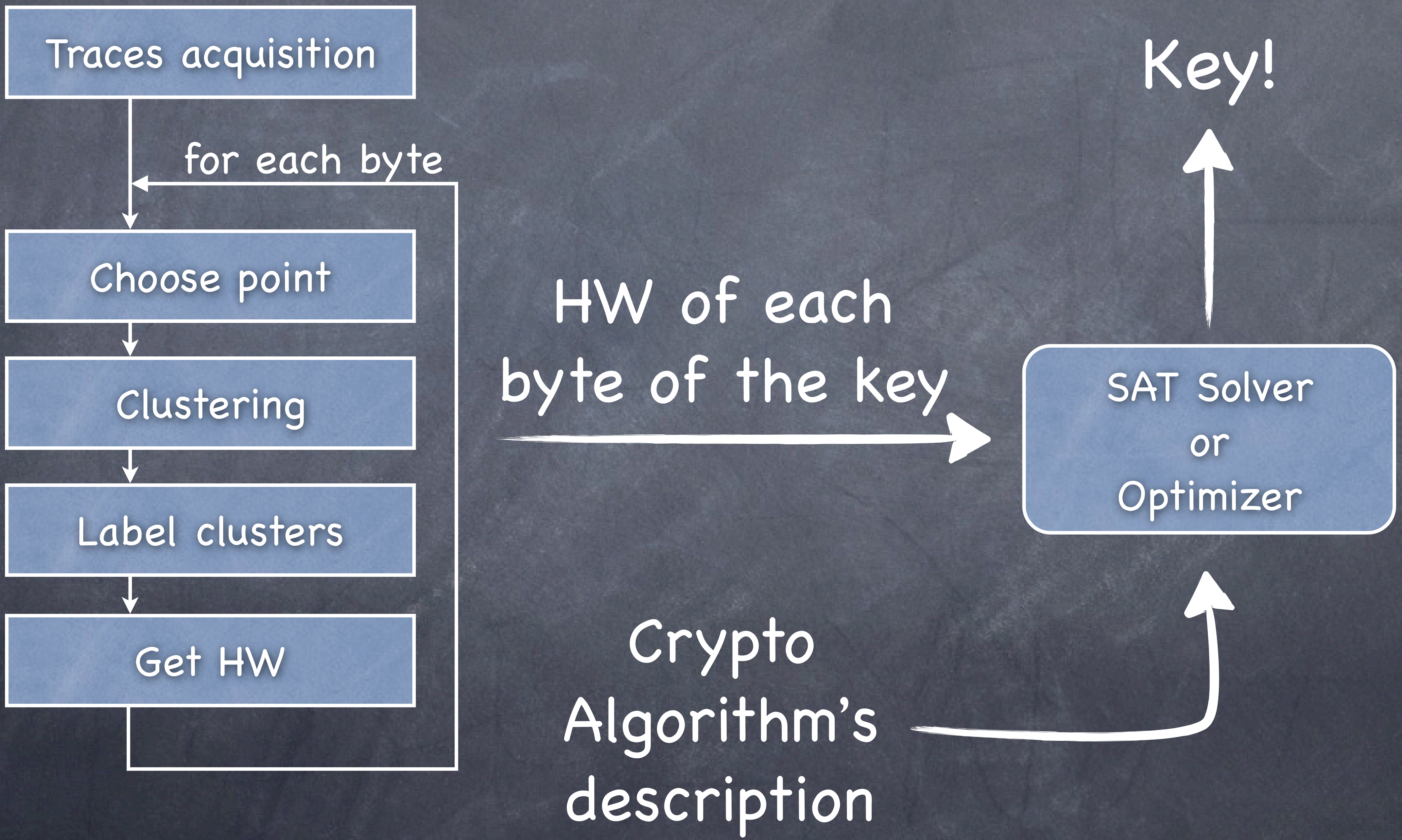


Getting the HW

We know the HW of each cluster!



Key recovery



Traces acquisition

for each byte

Choose point

Clustering

Label clusters

Get HW

HW of each byte of the key

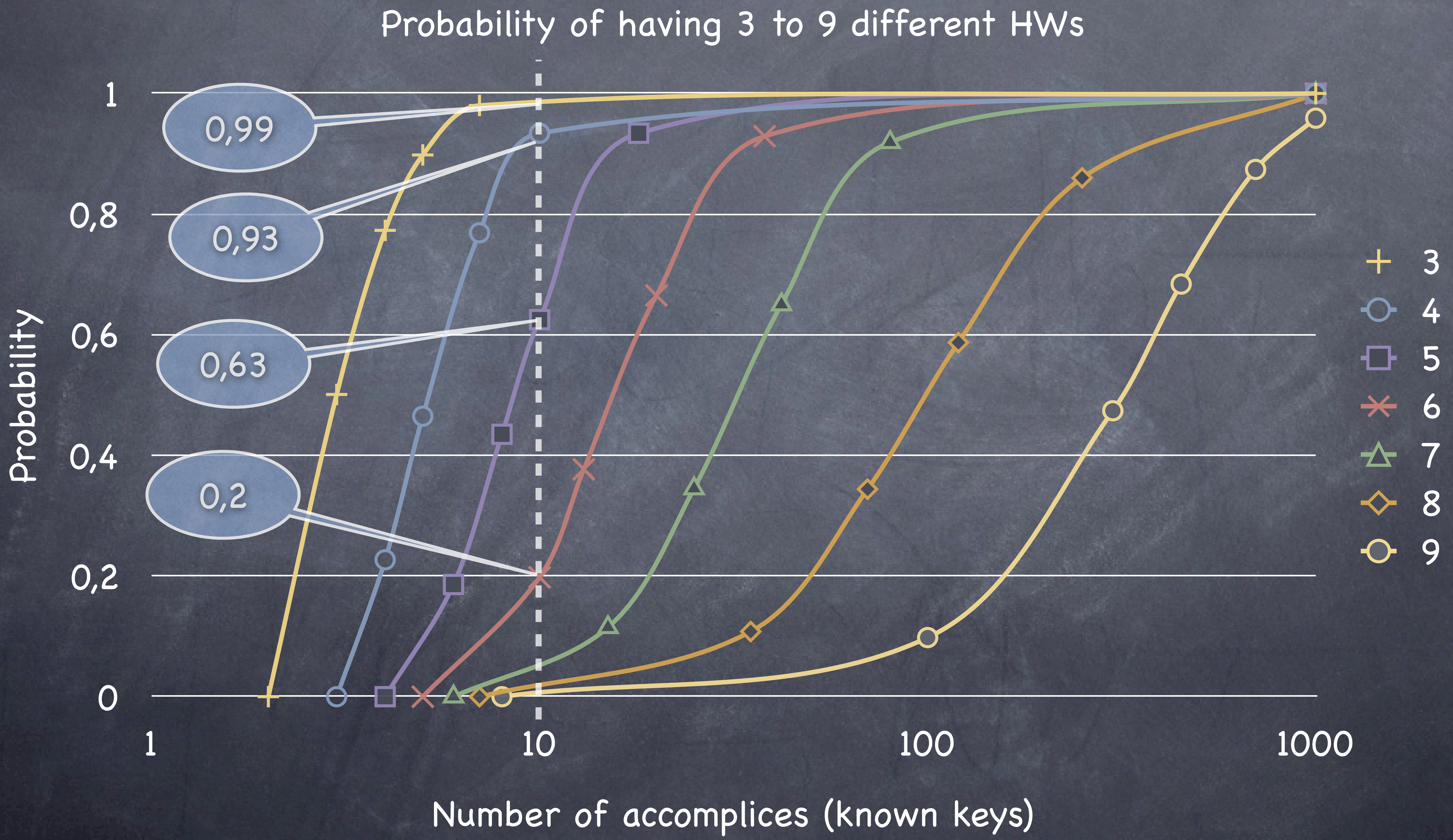
SAT Solver or Optimizer

Key!

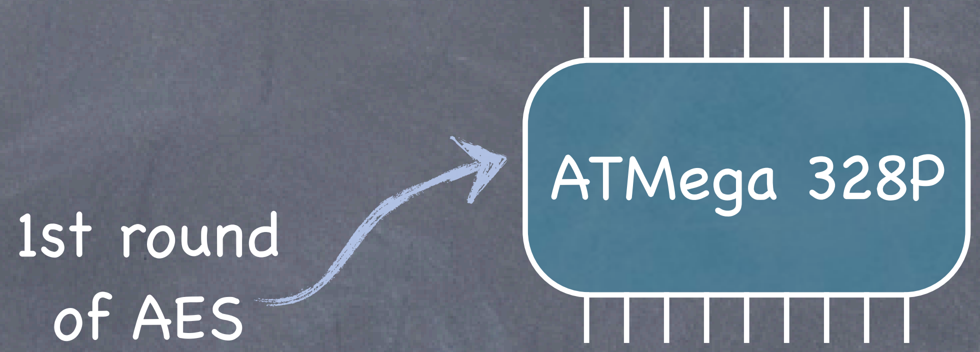
Crypto Algorithm's description

Simulations, Experiments & Discussion

Number of known keys



Experiment I



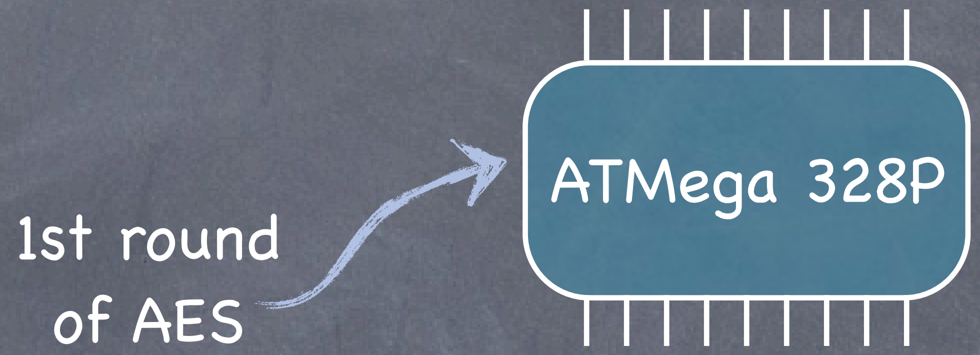
1st round
of AES

ATMega 328P

Attack	Success rate (%)
SSTA	62
Template Attack	84
Random Forest	78
Support Vector Machine	84
Simple model	27

- key : 0x00 except attacked byte
- plaintext : 0x00
- average of 128 traces
- all 256 values in the set U

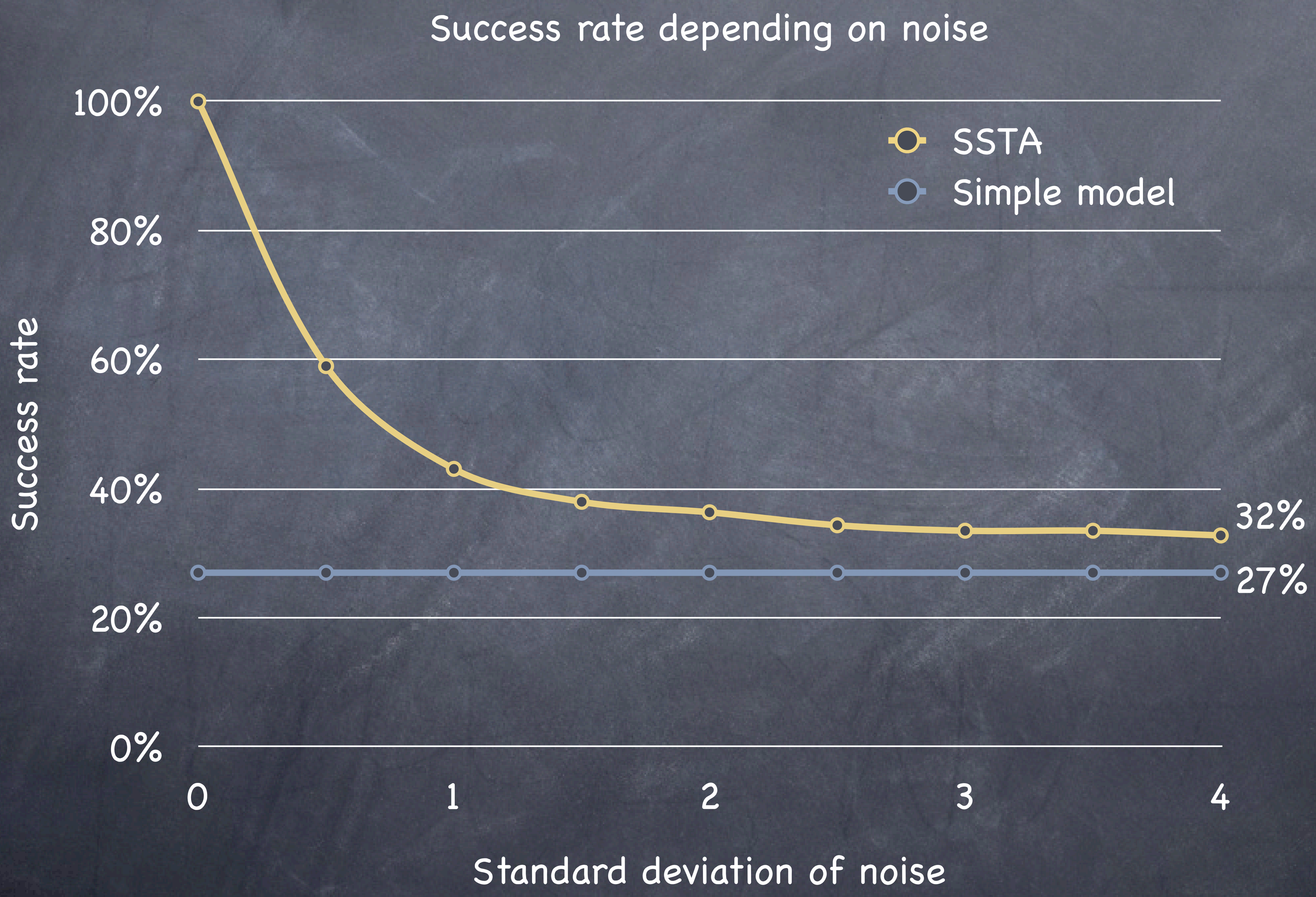
Experiment II



Attack	Success rate (%)
SSTA	53
Template Attack	72
Random Forest	73
Support Vector Machine	79
Simple model	27

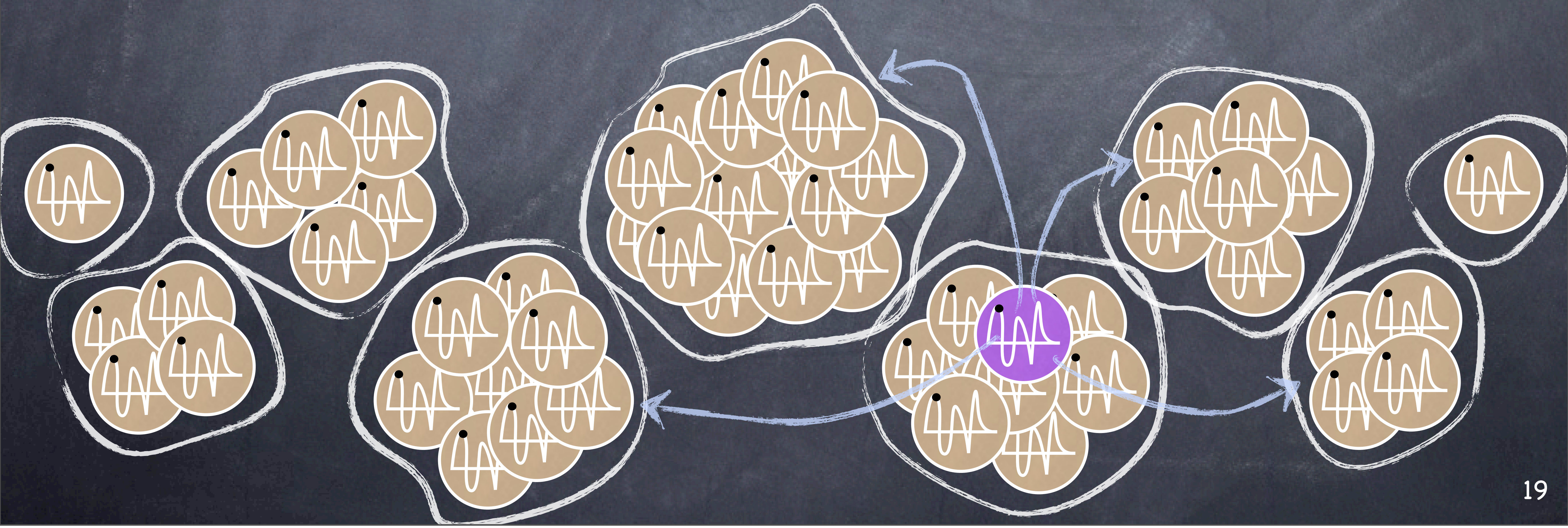
- key : random values
- plaintext : fixed random
- average of 100 traces
- 210 random values in the set U

Noise


Success rate depending on noise
SSTA
Simple model
Success rate
100%
80%
60%
40%
20%
0%
0
1
2
3
4
32%
27%
Standard deviation of noise

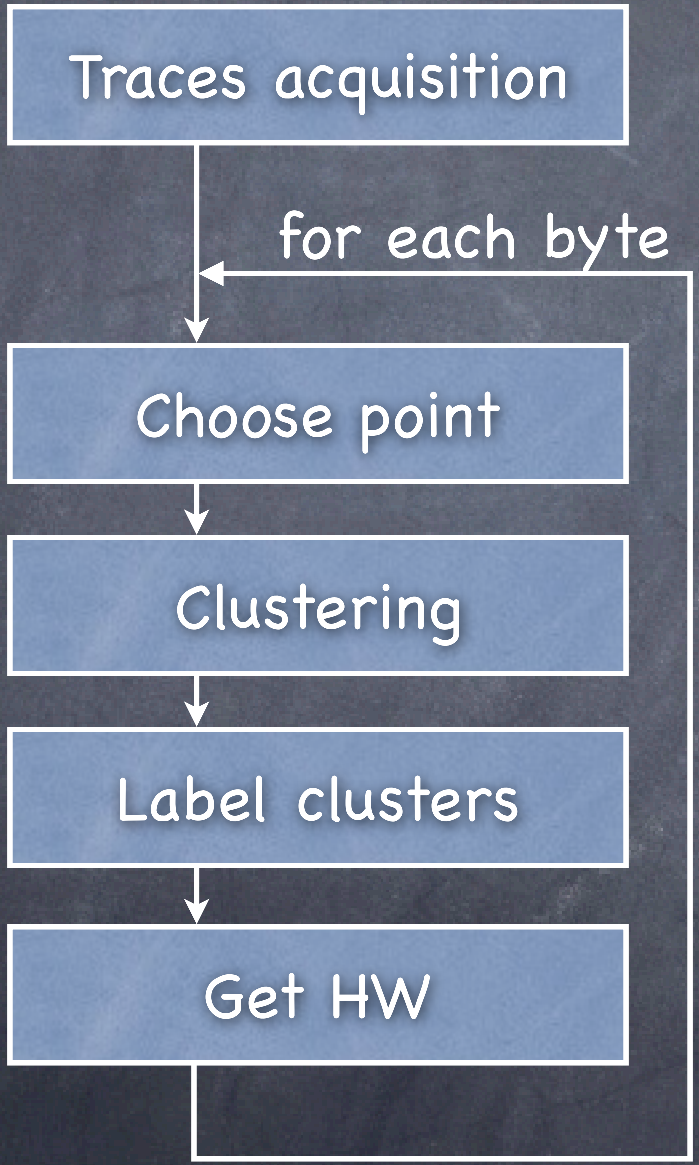
Clustering errors

SSTA	Success rate (%)		
	|HW-prediction|=0	|HW-prediction|<=1	|HW-prediction|<=2
Experiment I	62	90	100
Experiment II	53	85	100
Simple model	27	71	92



Conclusions & Future works

Conclusion



SSTA

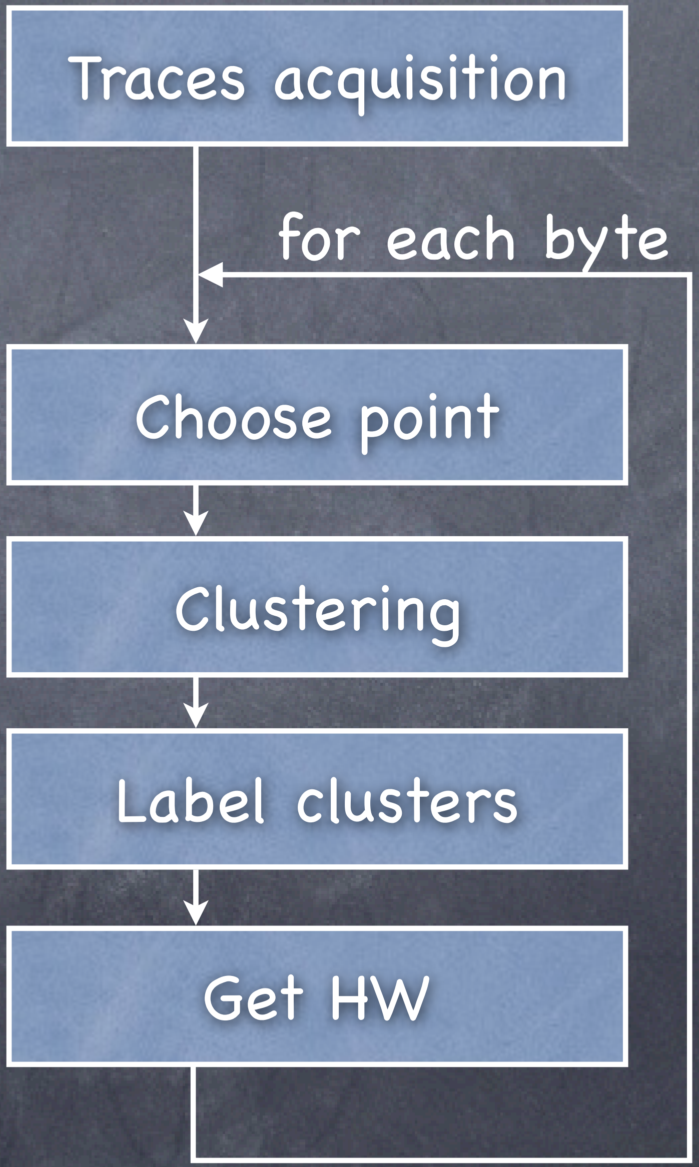
- Relaxes hypotheses
- Need few known keys
- Attack many power traces at a time
- Practical attack

Future works

- vary tools (dependency, clustering)
- adaptation to multivariate attacks
- study protected devices
- vary devices and crypto algorithms

The end

- http://www.ulb.ac.be/di/dpalab/
- http://qualsec.ulb.ac.be/
- nikita.veshchikov@ulb.be



Traces acquisition

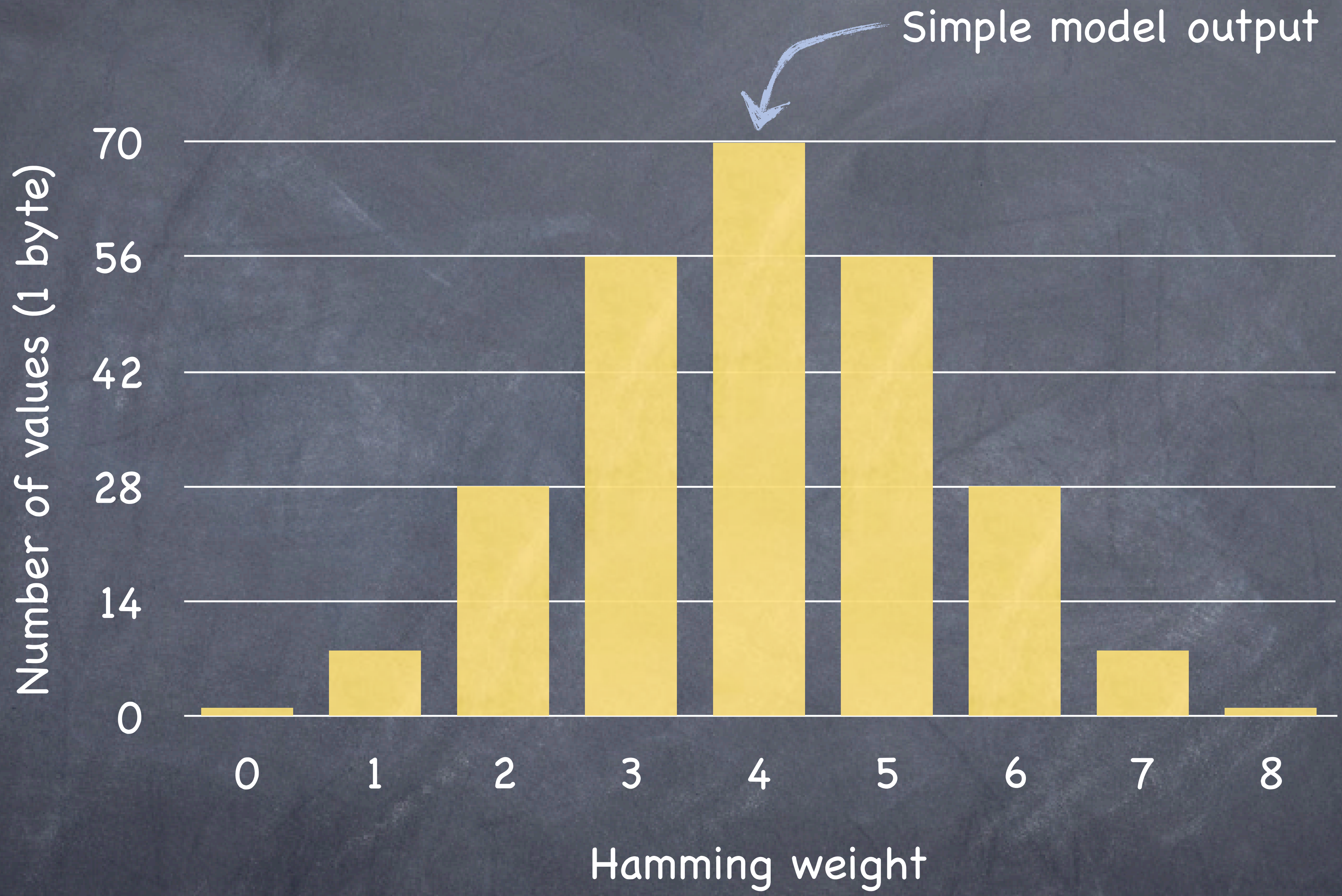
for each byte

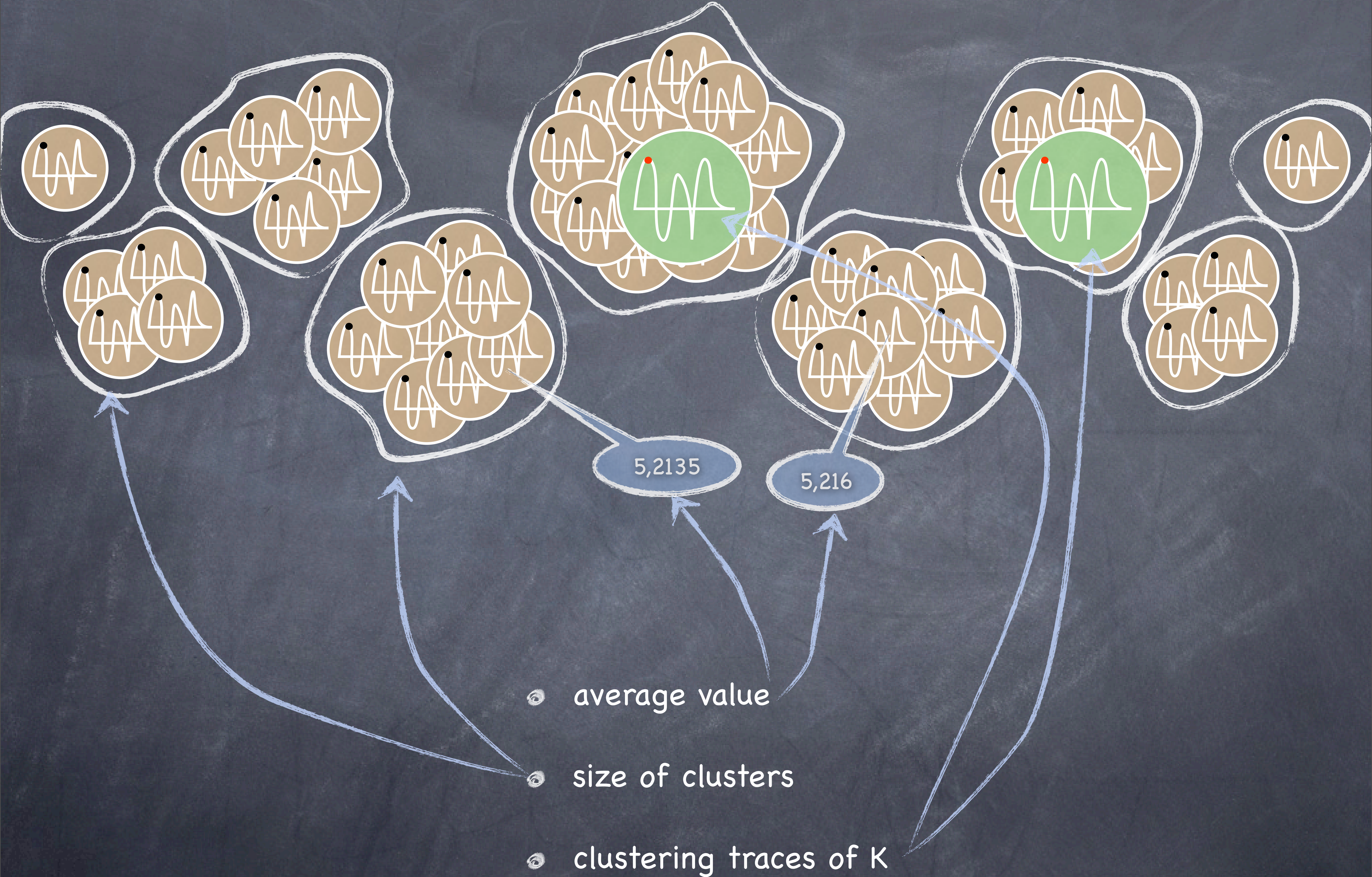
Choose point

Clustering

Label clusters

Get HW


Simple model output
Number of values (1 byte)
70
56
42
28
14
0
0
1
2
3
4
5
6
7
8
Hamming weight



- average value
- size of clusters
- clustering traces of K