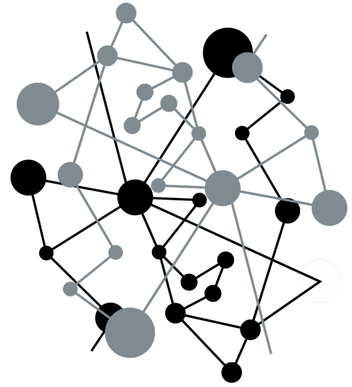


Learning when to stop

Ileana Buhan
@ileanabuhan

riscure

Our story..

2020

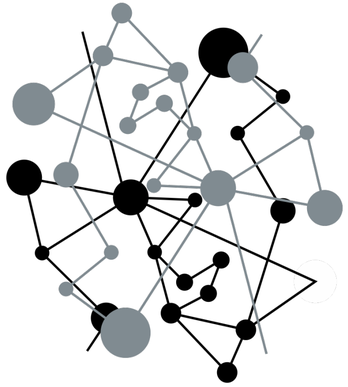
2017

2005

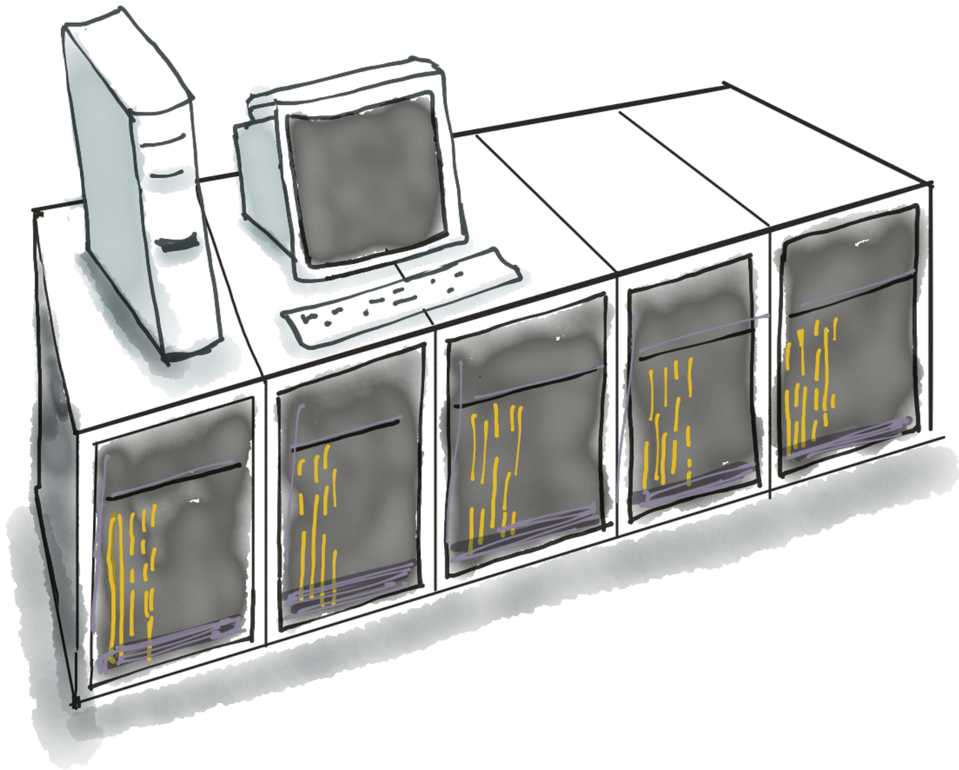
1997

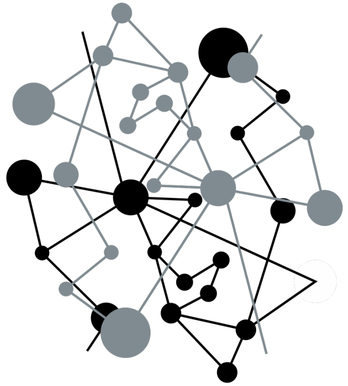
1941

Its 1941

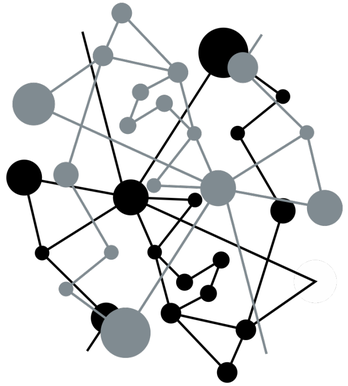


Its 1997…

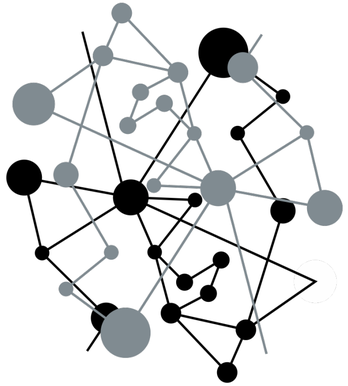


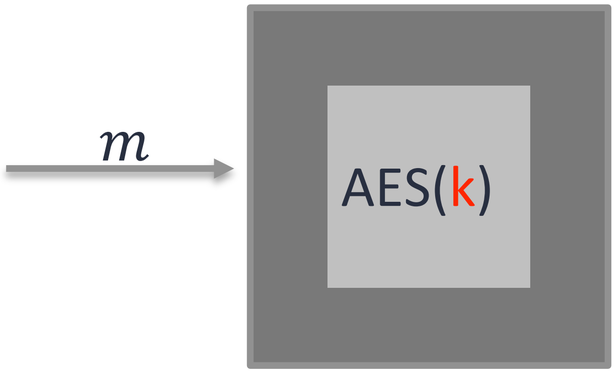


Its 2005…



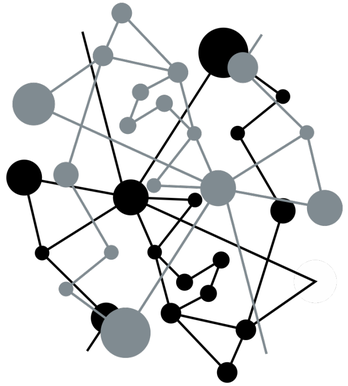
SCA (non-profiled)

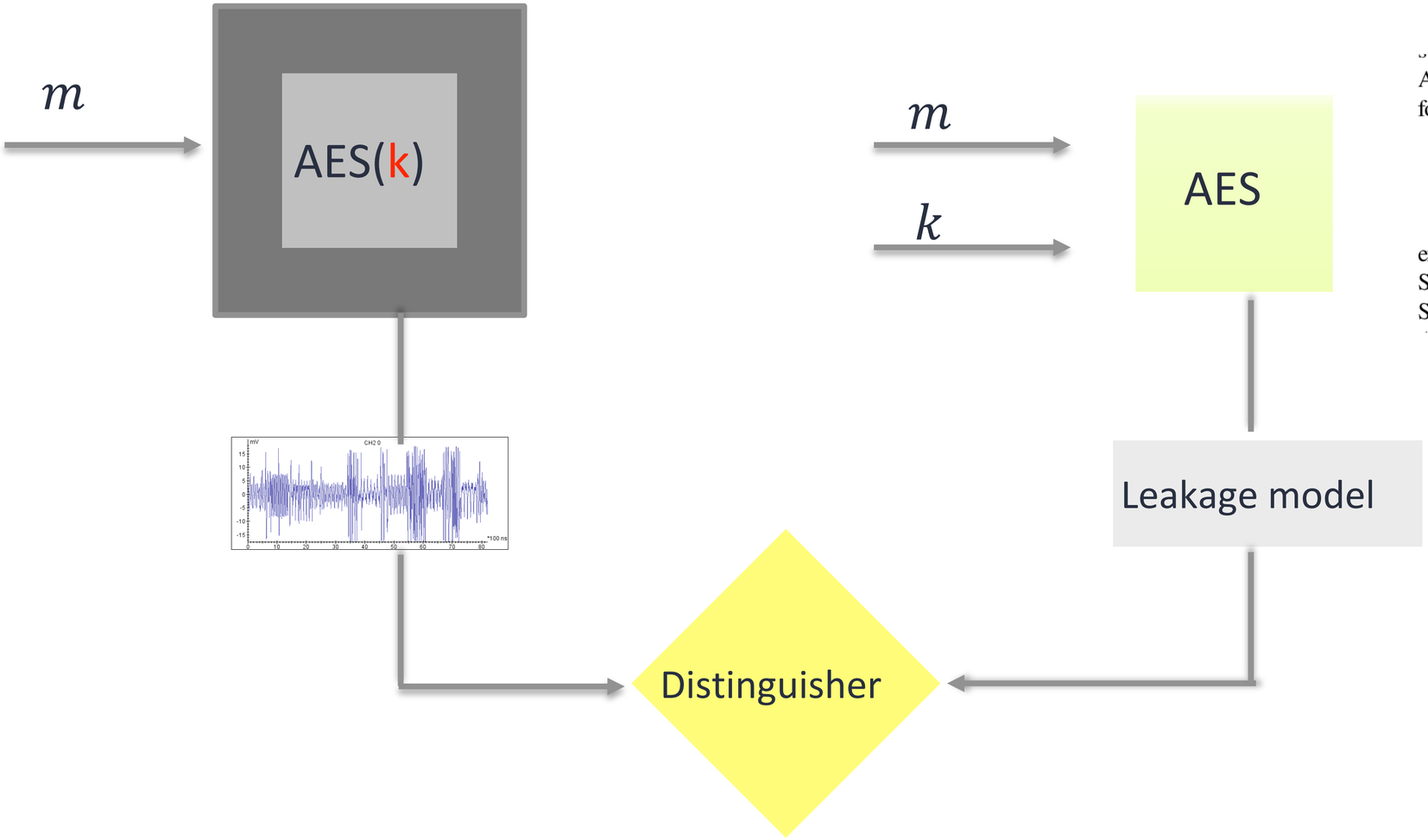




closed sample

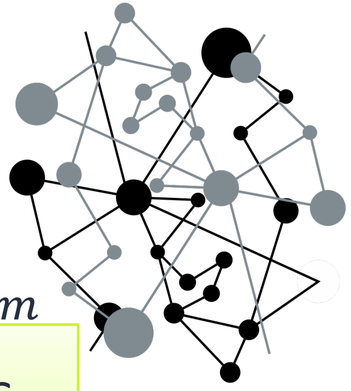
SCA (non-profiled)





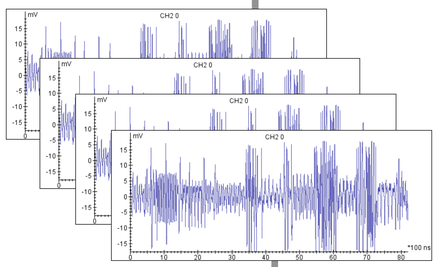

```
AddRoundKey(state, &w[0])
for i = 1 step 1 to 9
    SubBytes(state)
    ShiftRows(state)
    MixColumns(state)
    AddRoundKey(state, &w[i*4])
end for
SubBytes(state)
ShiftRows(state)
```

SCA (non-profiled)



$m_1, m_2, m_3 .. m_n$

AES(k)



k_1 k_2 k_3 k_m

m_1 AES m_1 AES m_1 AES m_1 AES

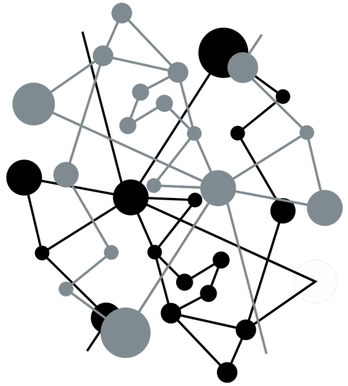
m_2 AES m_2 AES m_2 AES m_2 AES

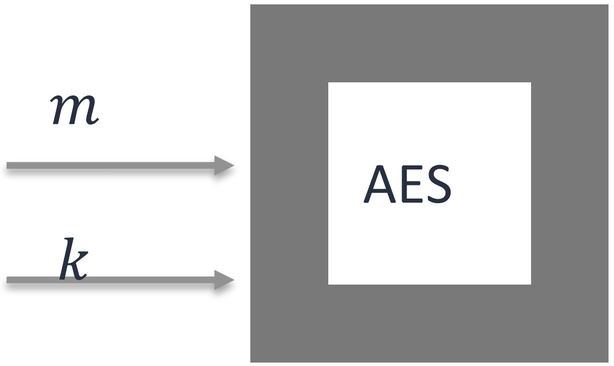
m_n AES m_n AES m_n AES m_n AES

$d(k_1)$ $d(k_2)$ $d(k_3)$ $d(k_m)$

$k_i \approx k$

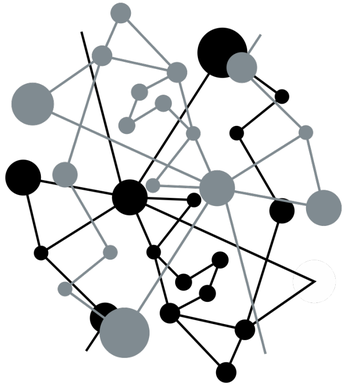
SCA (profiled)

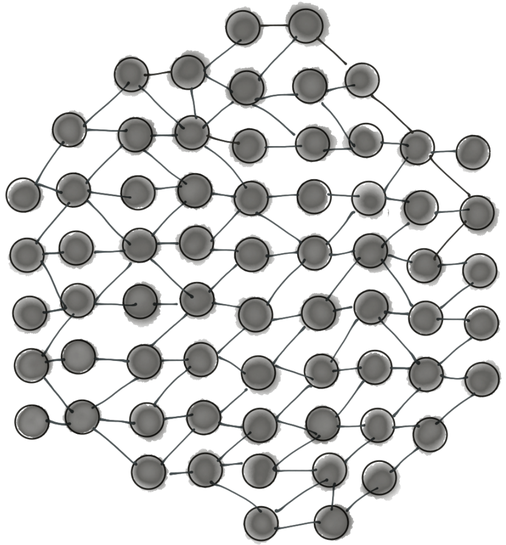




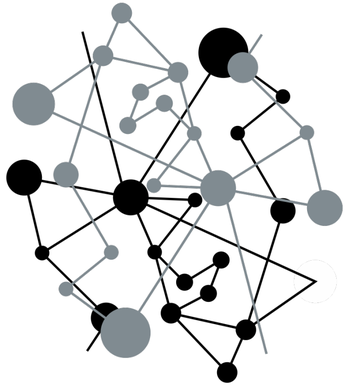
open sample

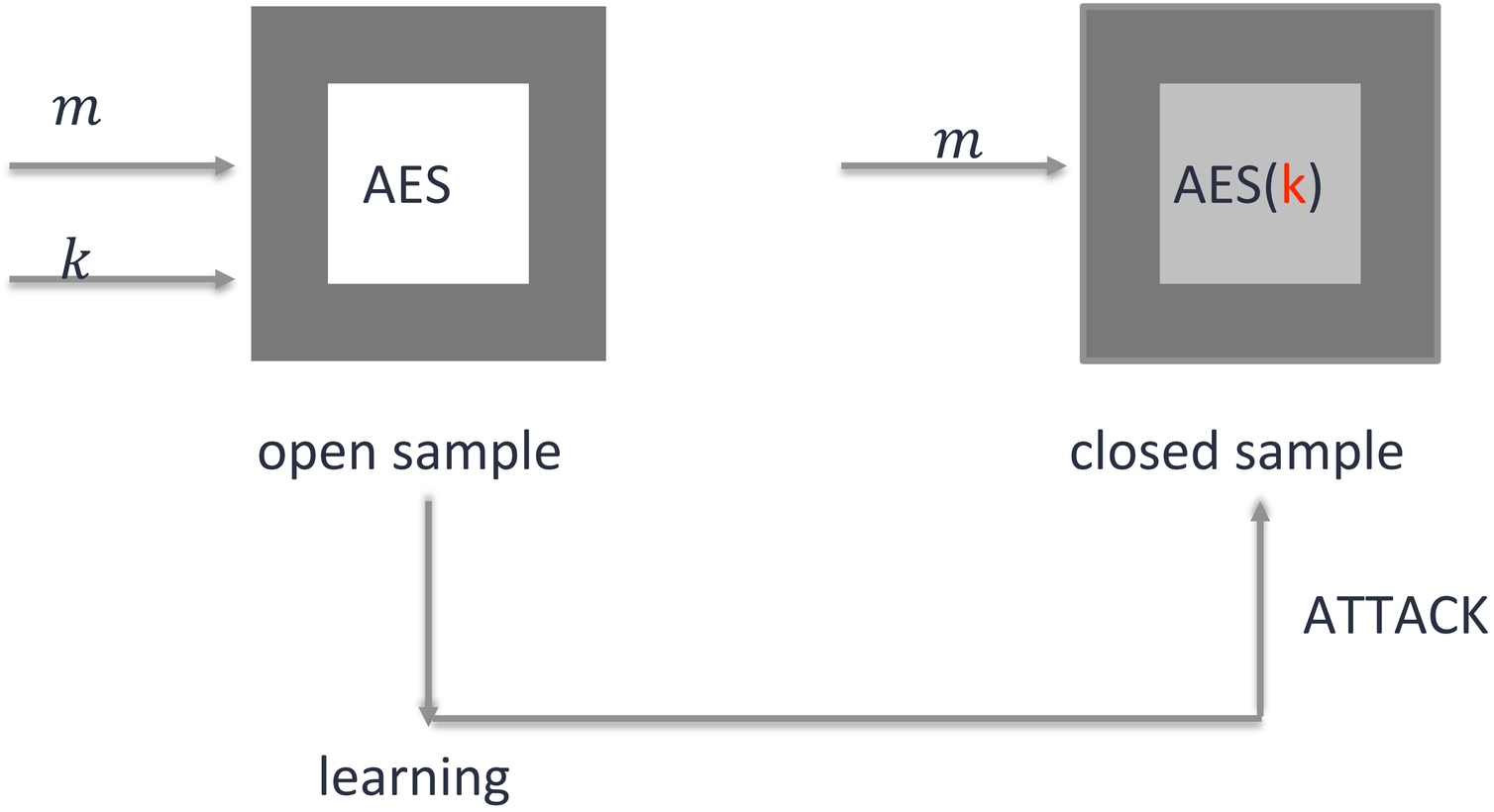
Its 2017



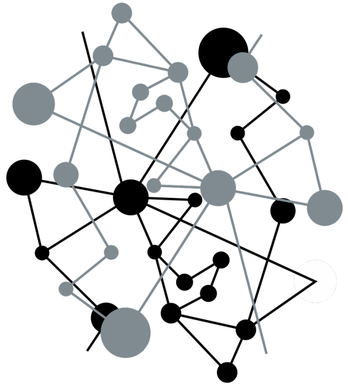


SCA (profiled)





Workflow



Acquisition

Learning/Profiling

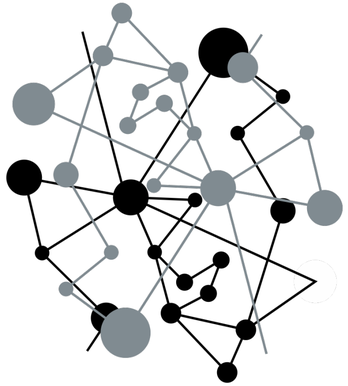
Attack

TRACES

BUILD the MACHINE

USE the MACHINE

Workflow



Acquisition

Learning/Profiling

Attack

TRACES

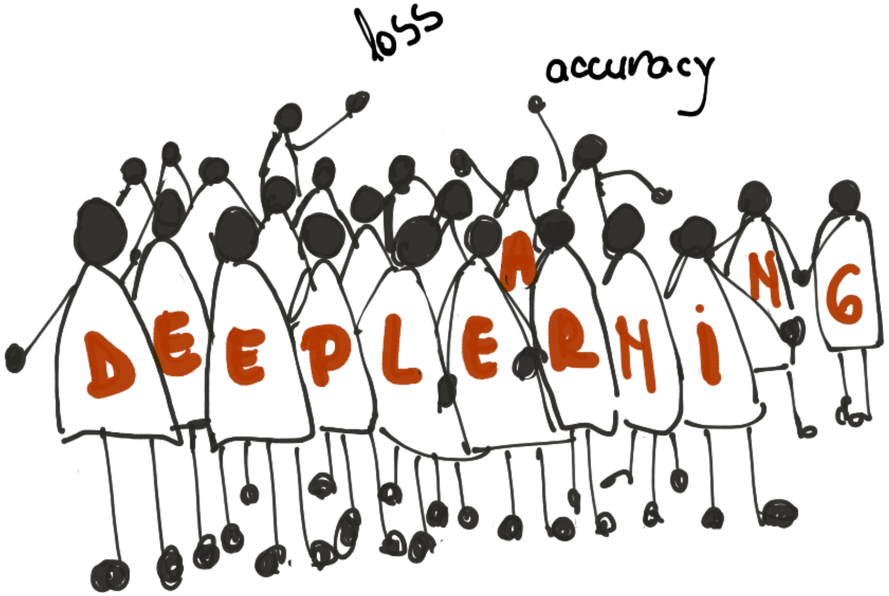
BUILD the MACHINE

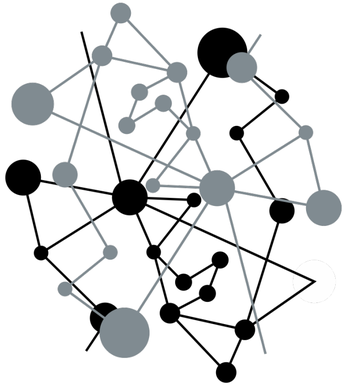
CONSTRUCT

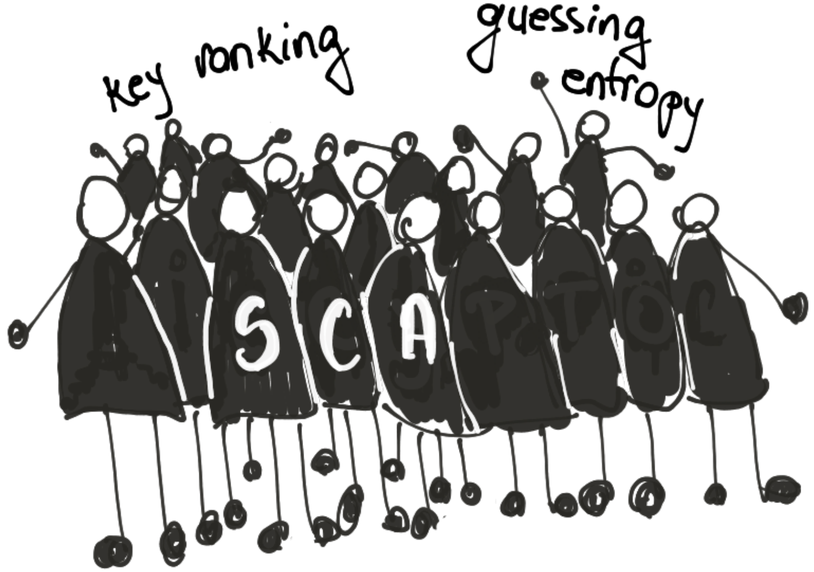
TRAIN

USE the MACHINE

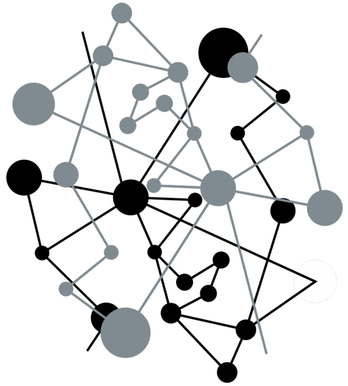
But..


loss
accuracy
DEEPLEARNING




key ranking
guessing entropy
SCA

Workflow



Acquisition

Learning/Profiling

Attack

TRACES

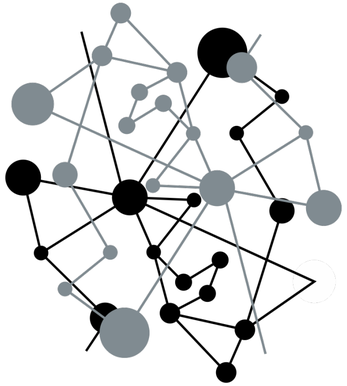
BUILD the MACHINE

CONSTRUCT

TRAIN

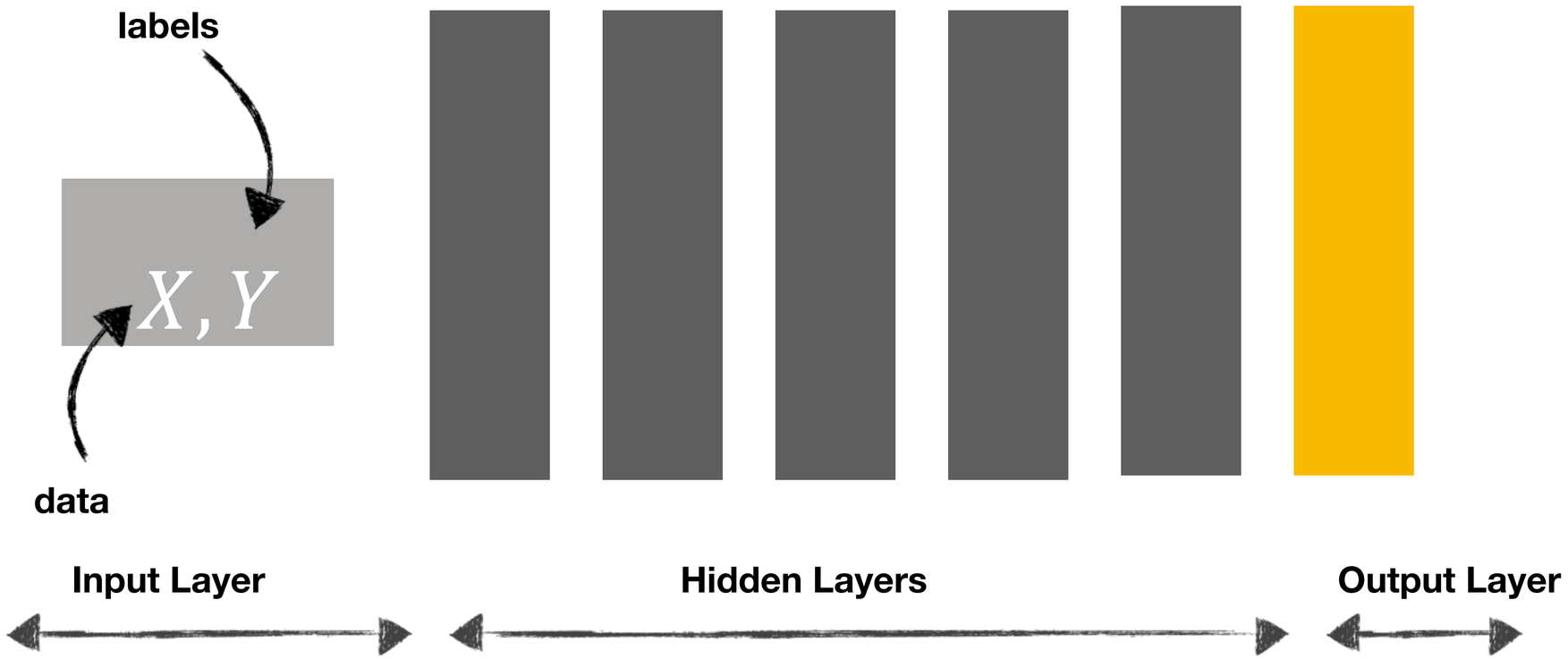
USE the MACHINE

But..



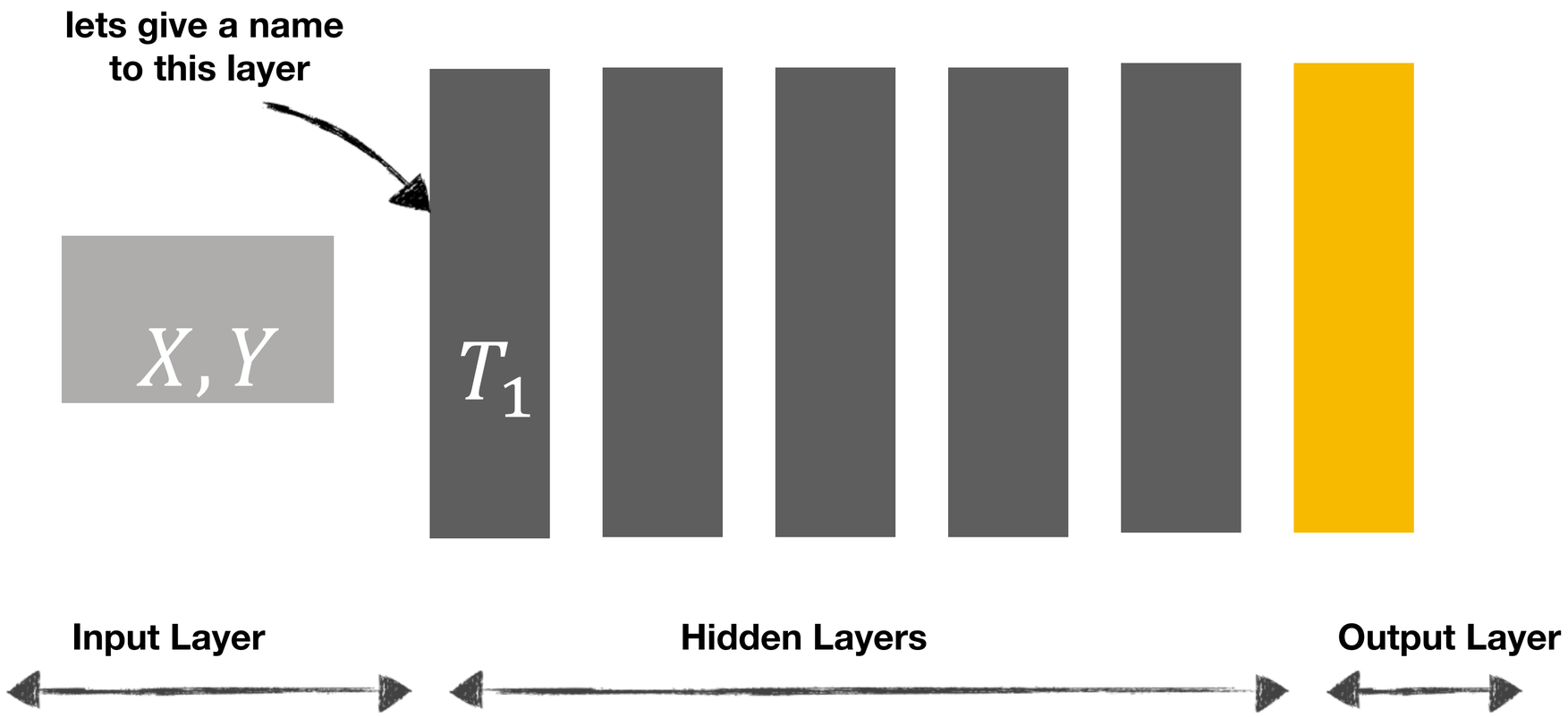
Perin G., Buhan I.R., Picek S., Learning when to stop:a mutual information approach to fight overfitting in profiled side-channel analysis a mutual information approach to fight overfitting in profiled side-channel analysis (Submitted to CHES 2020);

Leakage characterisation using deep networks

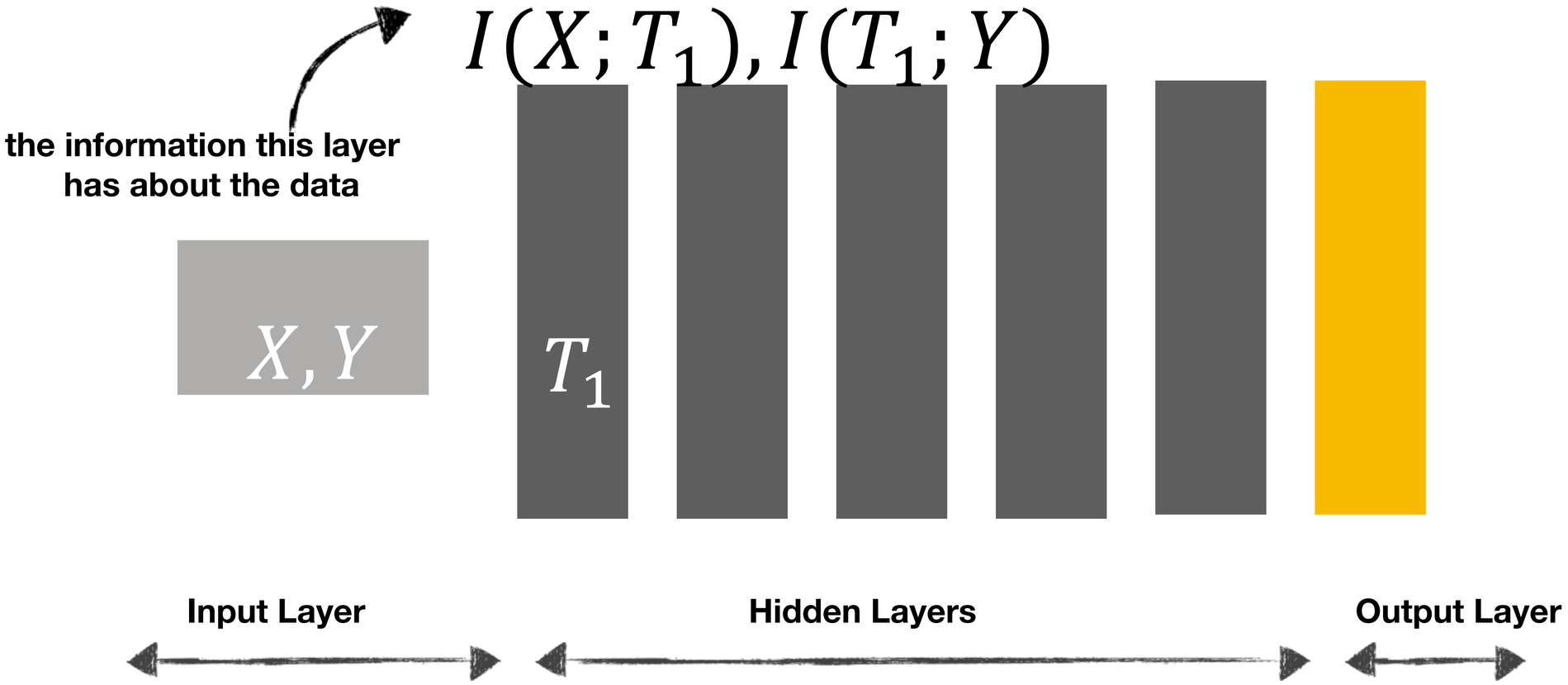


Perin G., Buhan I.R., Picek S., Learning when to stop:a mutual information approach to fight overfitting in profiled side-channel analysis a mutual information approach to fight overfitting in profiled side-channel analysis (Submitted to CHES 2020);

Leakage characterisation using deep networks

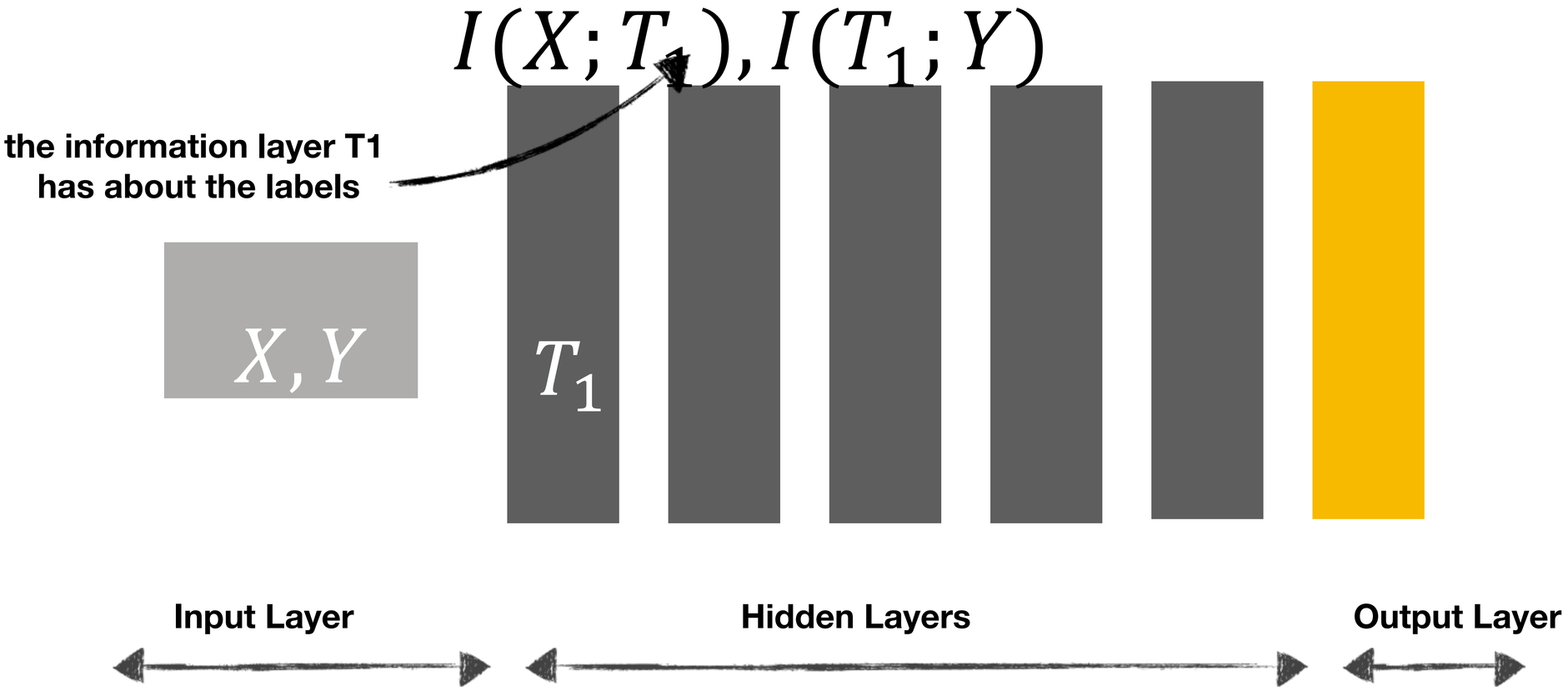


Leakage characterisation using deep networks



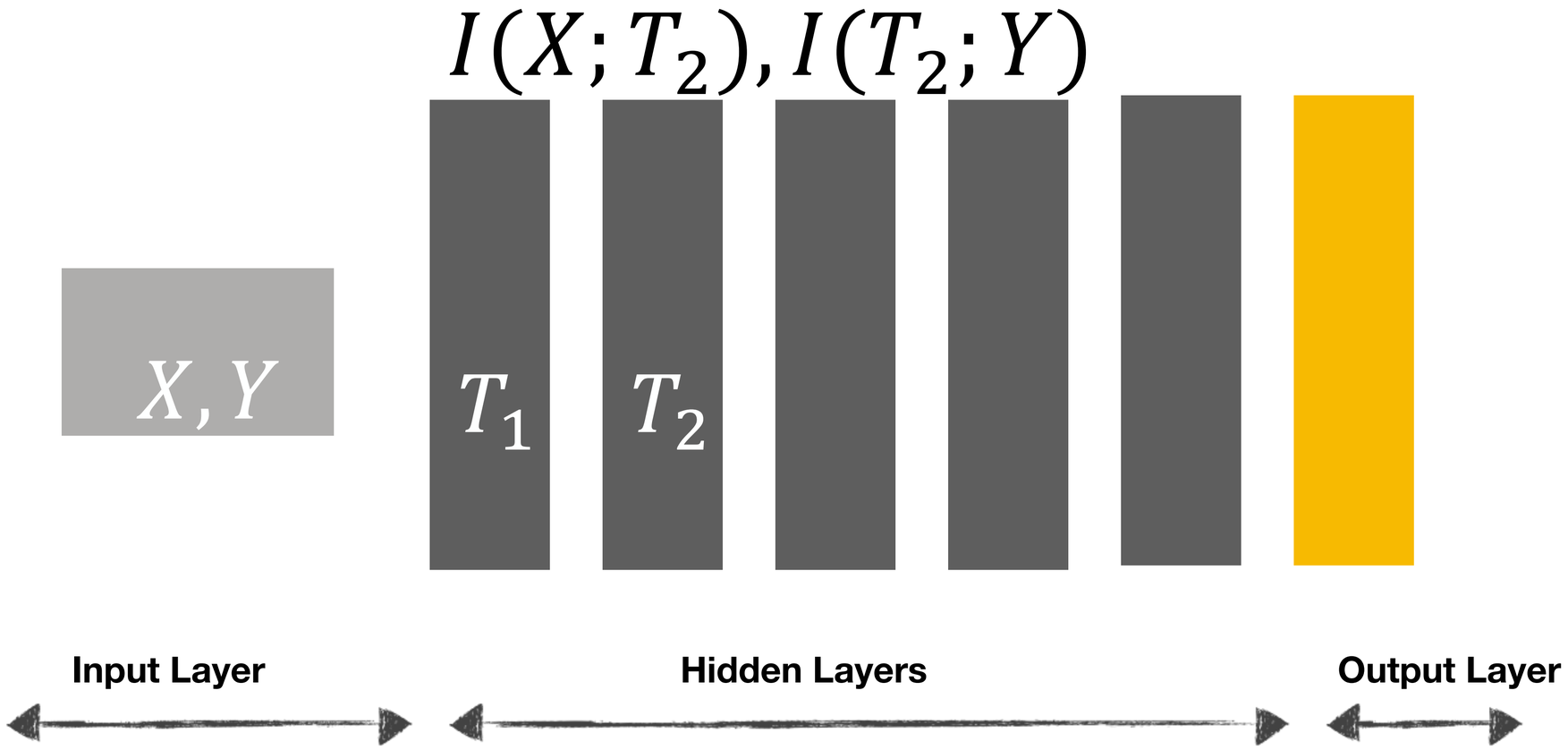
Perin G., Buhan I.R., Picek S., Learning when to stop:a mutual information approach to fight overfitting in profiled side-channel analysis a mutual information approach to fight overfitting in profiled side-channel analysis (Submitted to CHES 2020);

Leakage characterisation using deep networks



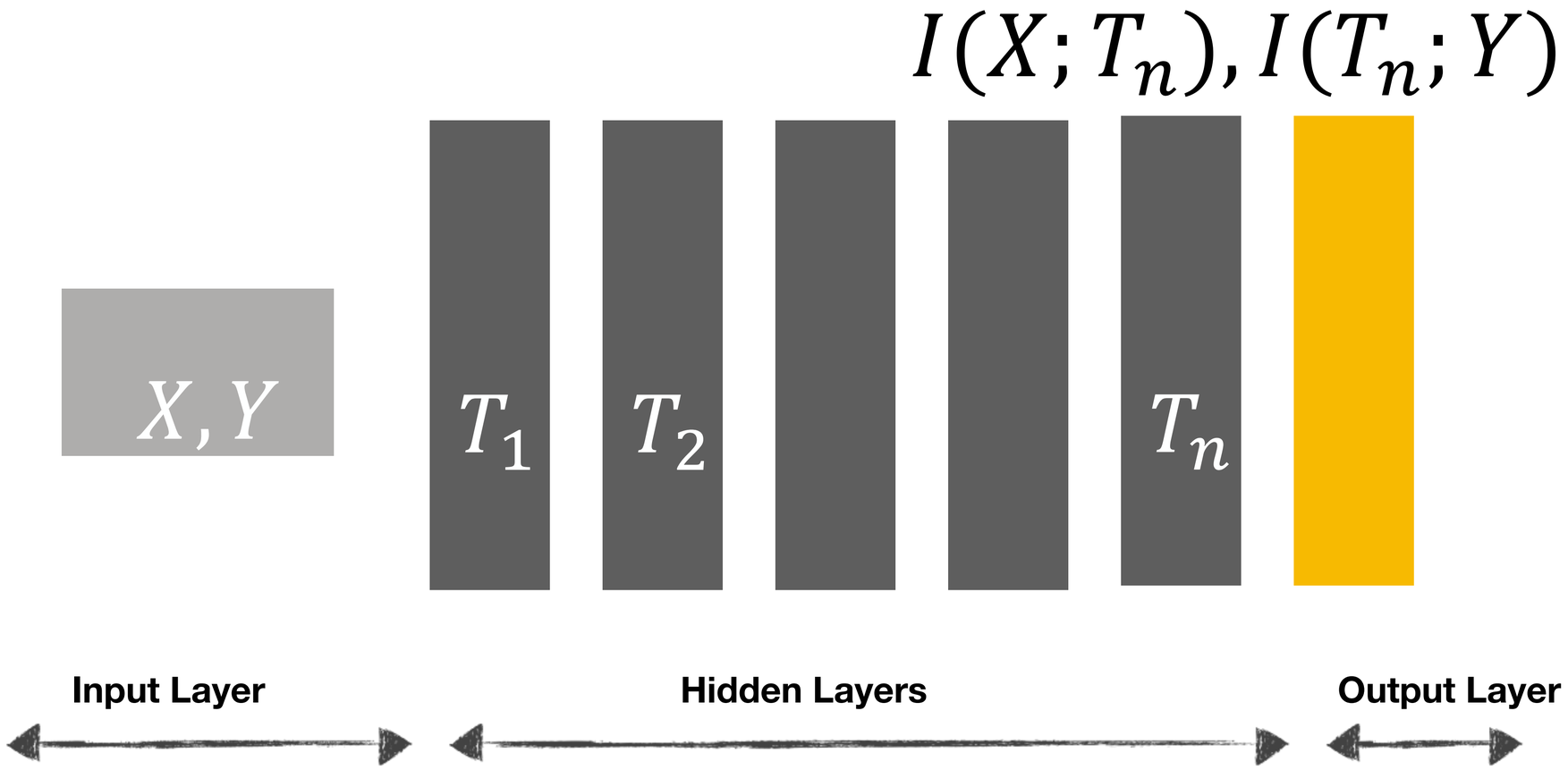
Perin G., Buhan I.R., Picek S., Learning when to stop:a mutual information approach to fight overfitting in profiled side-channel analysis a mutual information approach to fight overfitting in profiled side-channel analysis (Submitted to CHES 2020);

Leakage characterisation using deep networks



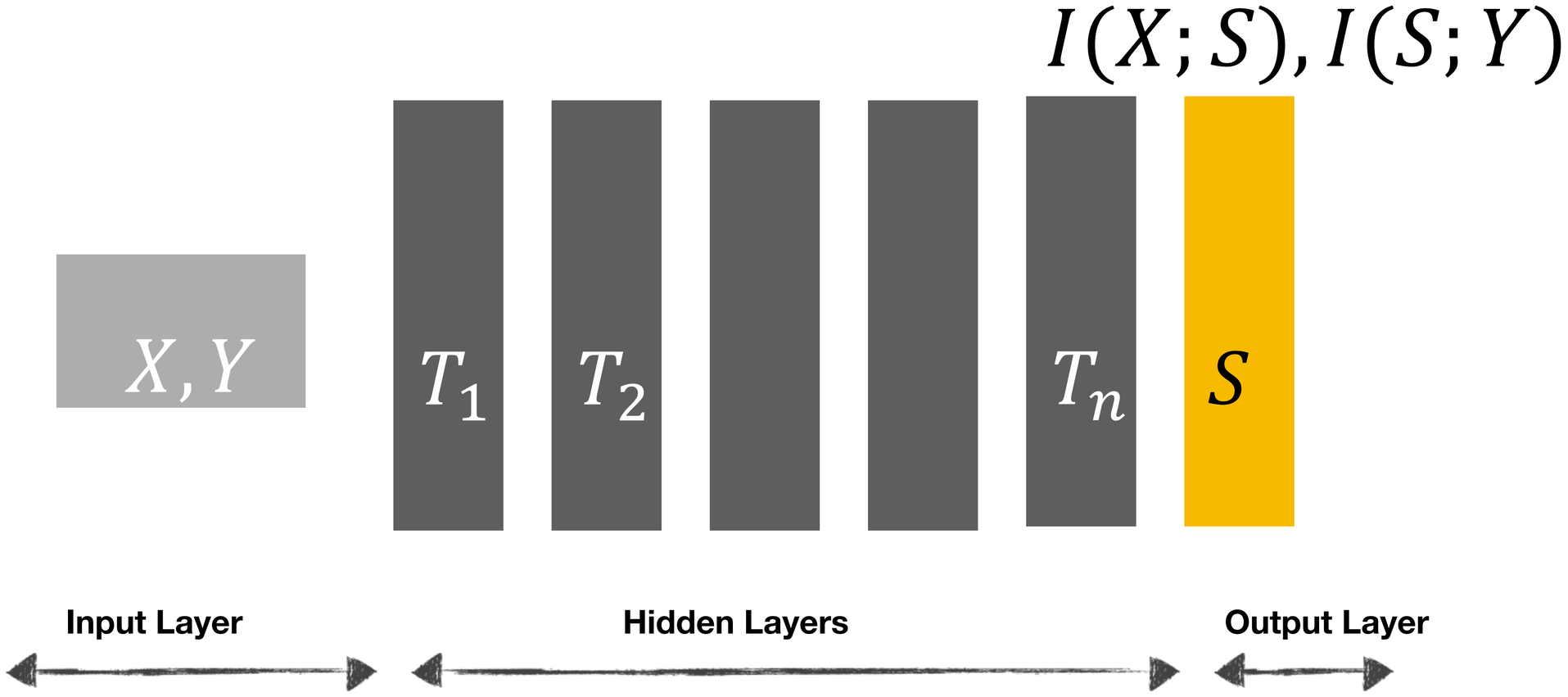
Perin G., Buhan I.R., Picek S., Learning when to stop:a mutual information approach to fight overfitting in profiled side-channel analysis a mutual information approach to fight overfitting in profiled side-channel analysis (Submitted to CHES 2020);

Leakage characterisation using deep networks



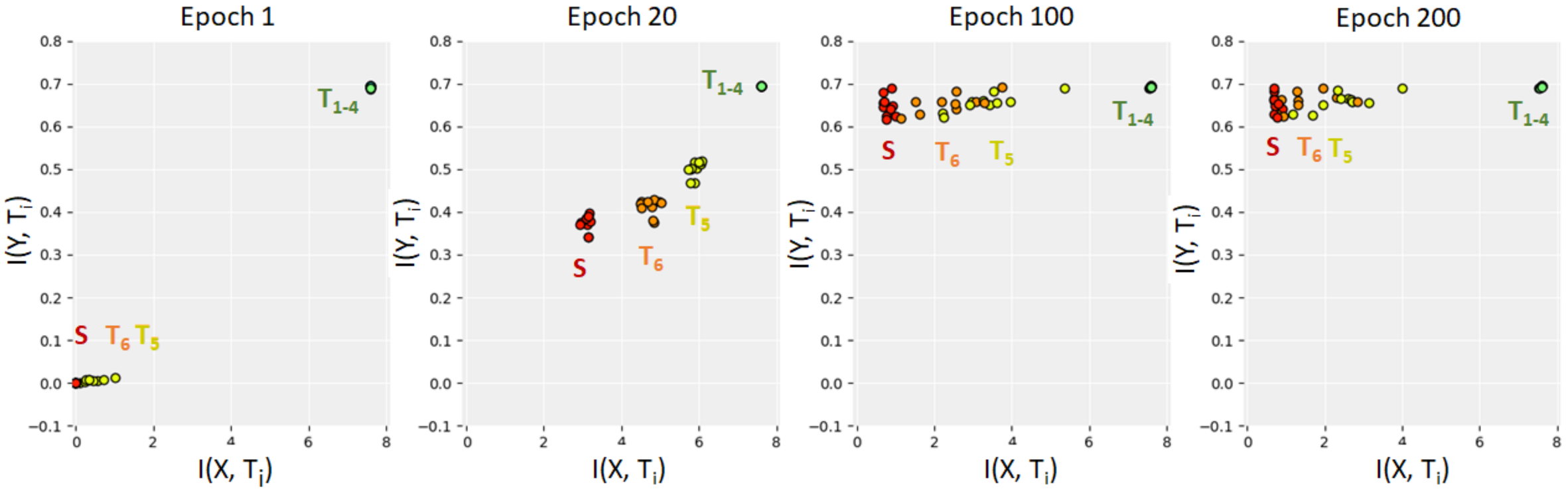
Perin G., Buhan I.R., Picek S., Learning when to stop:a mutual information approach to fight overfitting in profiled side-channel analysis a mutual information approach to fight overfitting in profiled side-channel analysis (Submitted to CHES 2020);

Leakage characterisation using deep networks



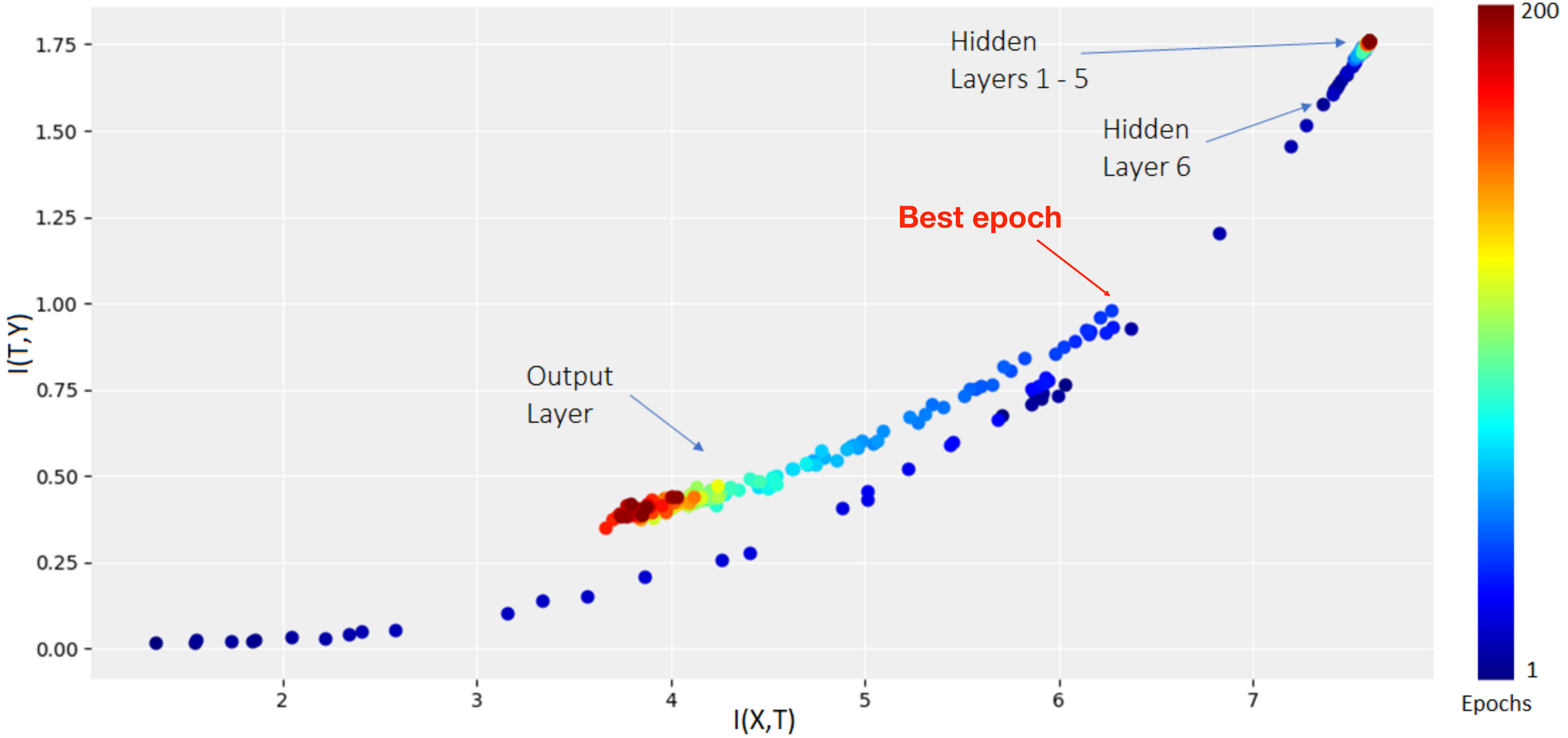
Perin G., Buhan I.R., Picek S., Learning when to stop:a mutual information approach to fight overfitting in profiled side-channel analysis a mutual information approach to fight overfitting in profiled side-channel analysis (Submitted to CHES 2020);

How a network learns



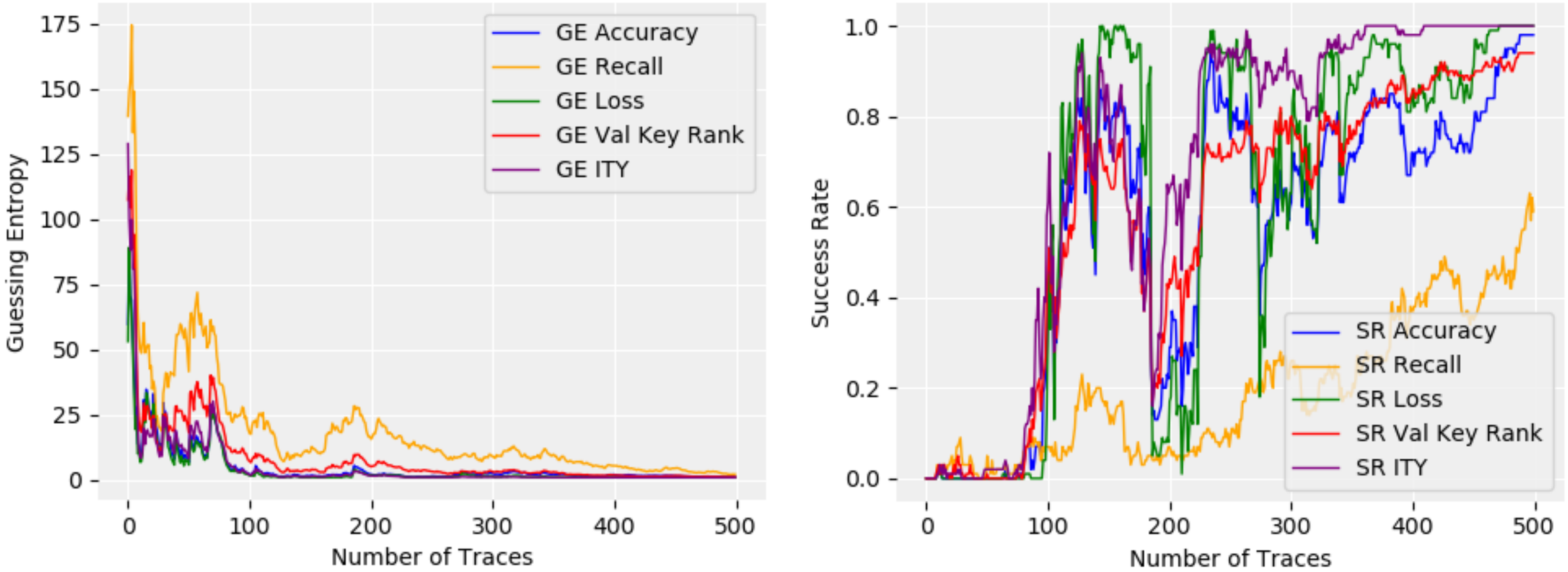
Perin G., Buhan I.R., Picek S., Learning when to stop:a mutual information approach to fight overfitting in profiled side-channel analysis a mutual information approach to fight overfitting in profiled side-channel analysis (Submitted to CHES 2020);

How the network learns



validation set

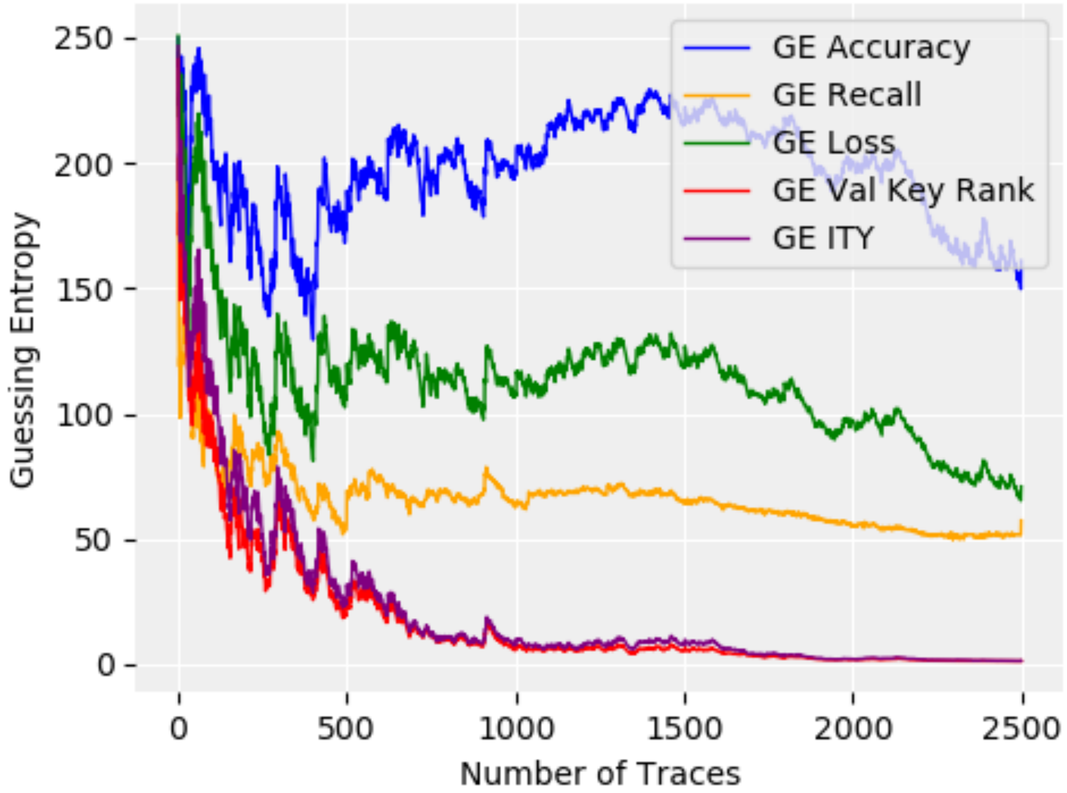
Leakage characterisation using deep networks

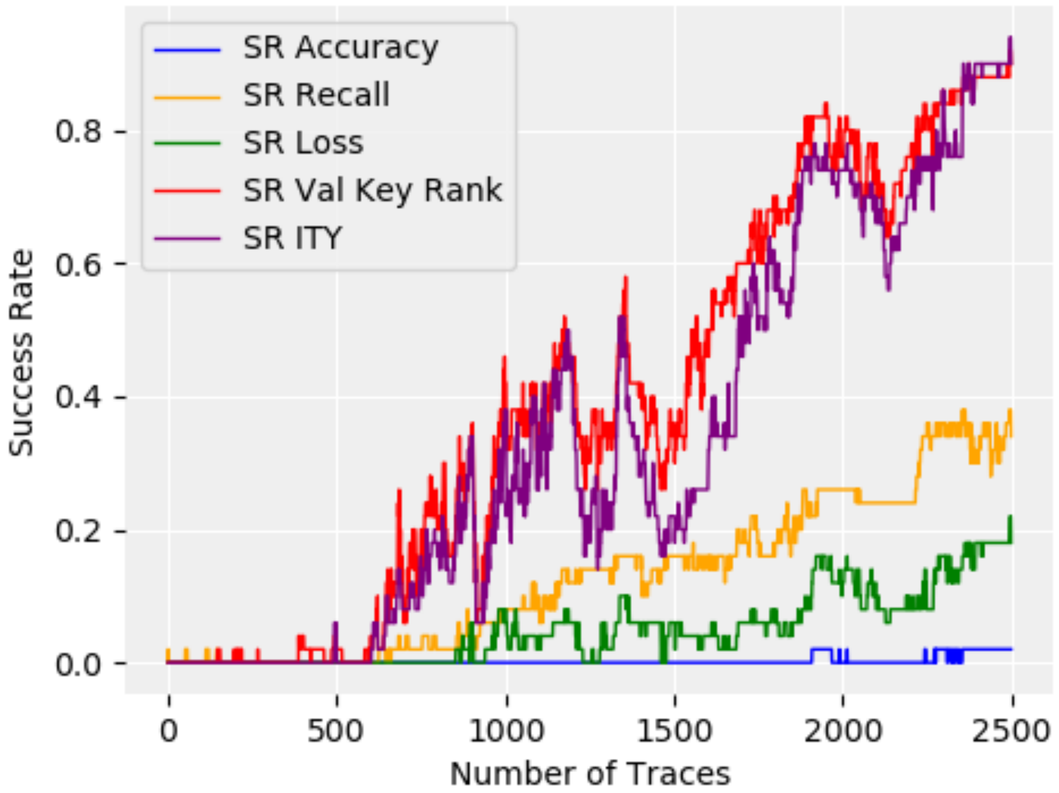


GE AND Success Rate on ASCAD database

Perin G., Buhan I.R., Picek S., Learning when to stop:a mutual information approach to fight overfitting in profiled side-channel analysis a mutual information approach to fight overfitting in profiled side-channel analysis (Submitted to CHES 2020);

Leakage characterisation using deep networks





GE AND Success Rate on CHES AES database

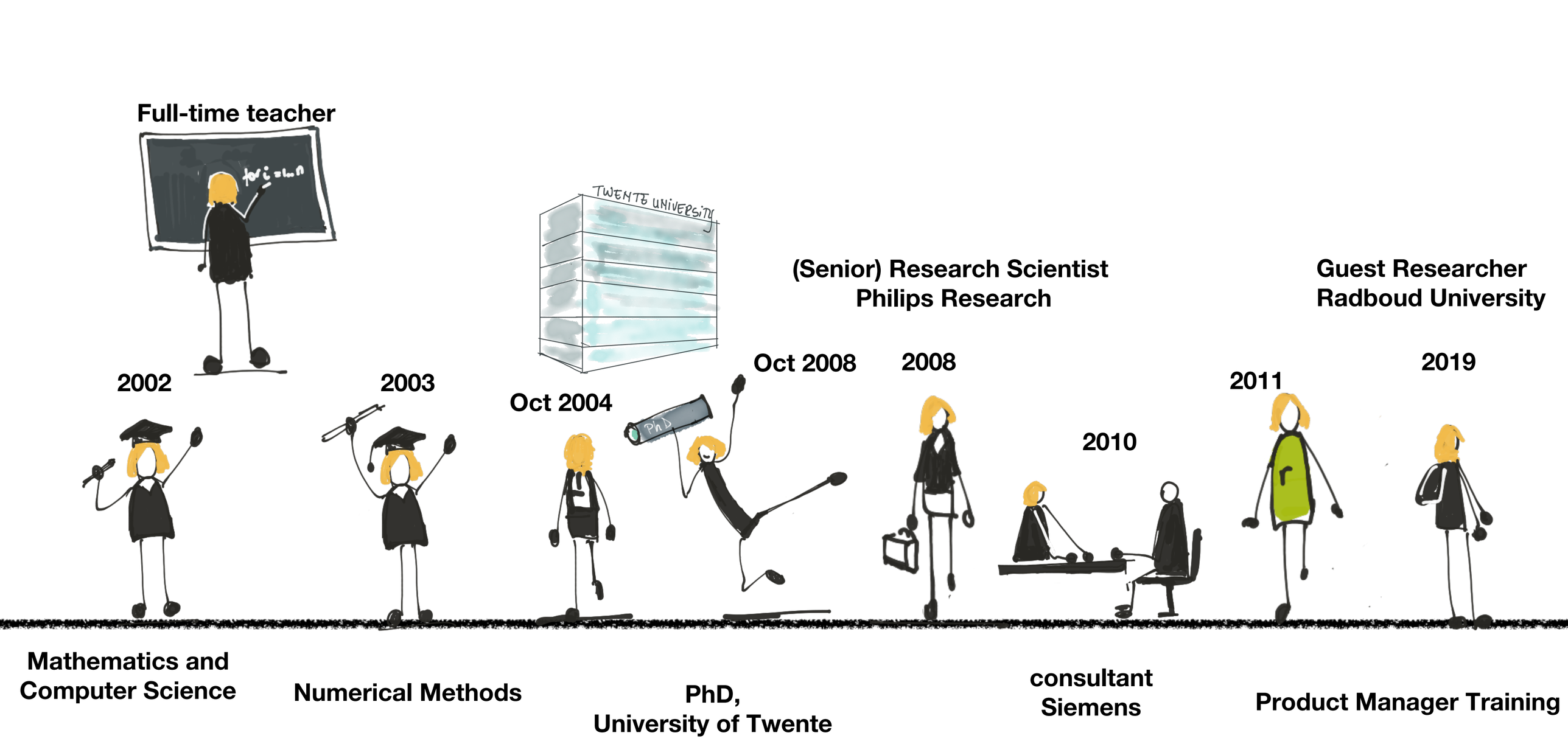
Perin G., Buhan I.R., Picek S., Learning when to stop:a mutual information approach to fight overfitting in profiled side-channel analysis a mutual information approach to fight overfitting in profiled side-channel analysis (Submitted to CHES 2020);

Message to my younger self

never stop being the your best version

never stop believing in yourself

help Jane *with security evaluations*


Full-time teacher
for i = 1 to n
TWENTE UNIVERSITY
PhD
(Senior) Research Scientist
Philips Research
Guest Researcher
Radboud University
2002
2003
Oct 2004
Oct 2008
2008
2010
2011
2019
Mathematics and
Computer Science
Numerical Methods
PhD,
University of Twente
consultant
Siemens
Product Manager Training