Reinforcement Learning for Hyperparameter Tuning in Deep Learning-based Side-channel Analysis

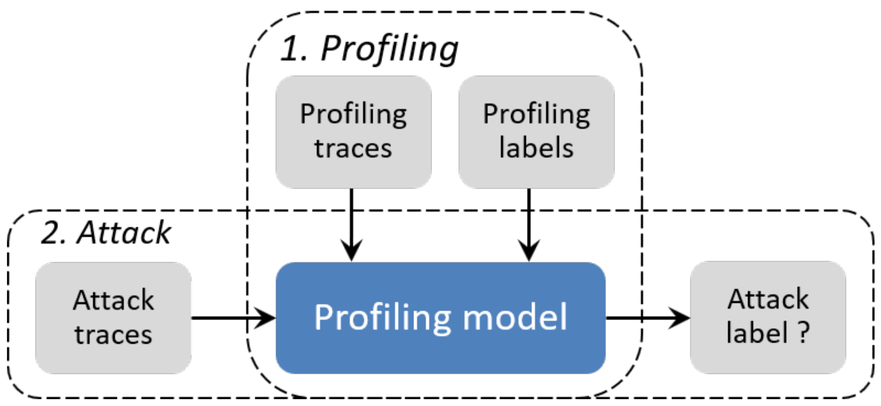
Jorai Rijsdijk[1], Lichao Wu[1], Guilherme Perin[2, 1] and Stjepan Picek[2, 1]

[1]Delft University of Technology, The Netherlands
[2]Radboud University, The Netherlands

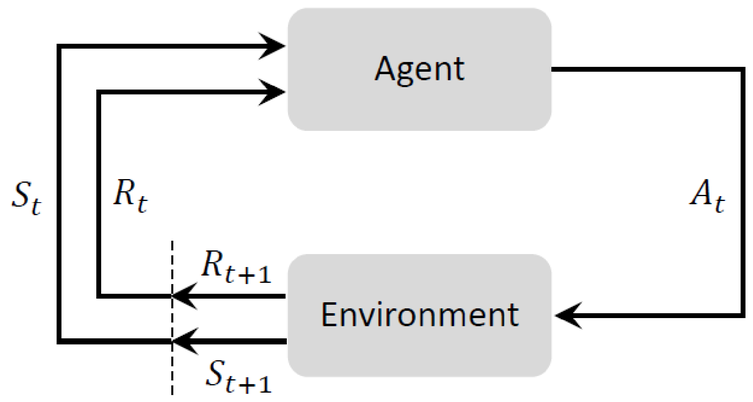
Introduction

Deep learning represents a powerful set of techniques for profiling side-channel analysis. However,

- Deep learning techniques commonly have a plethora of hyperparameters to tune
- Top DL-based attack results can come with a high price in preparing the attack.

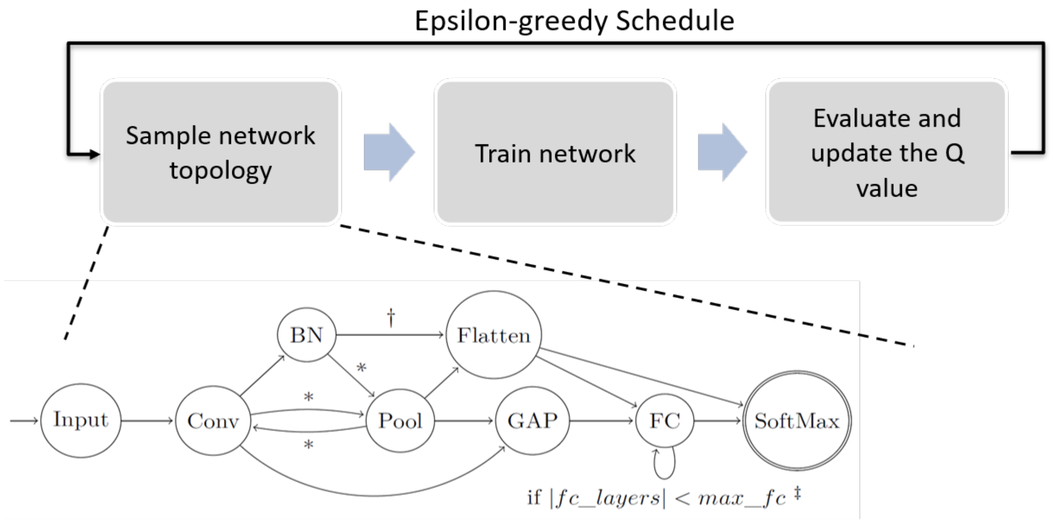


In this work, we propose to use reinforcement learning to automate the tuning of the hyperparameters.



Methodology

The algorithm considers the task of using Q-Learning in training an agent to sequentially choosing neural network layers and their hyperparameters.



When reaching a termination state, the algorithm evaluates the performance of the generated neural networks with a reward function.

$$R = \frac{t' + GE'_{10} + 0.5 \cdot GE'_{50} + 0.5 \cdot \alpha + p'}{4}$$

$$t' = \frac{t_{\max} - \min(t_{\max}, \overline{Q_{t_{GE}}})}{t_{\max}}$$

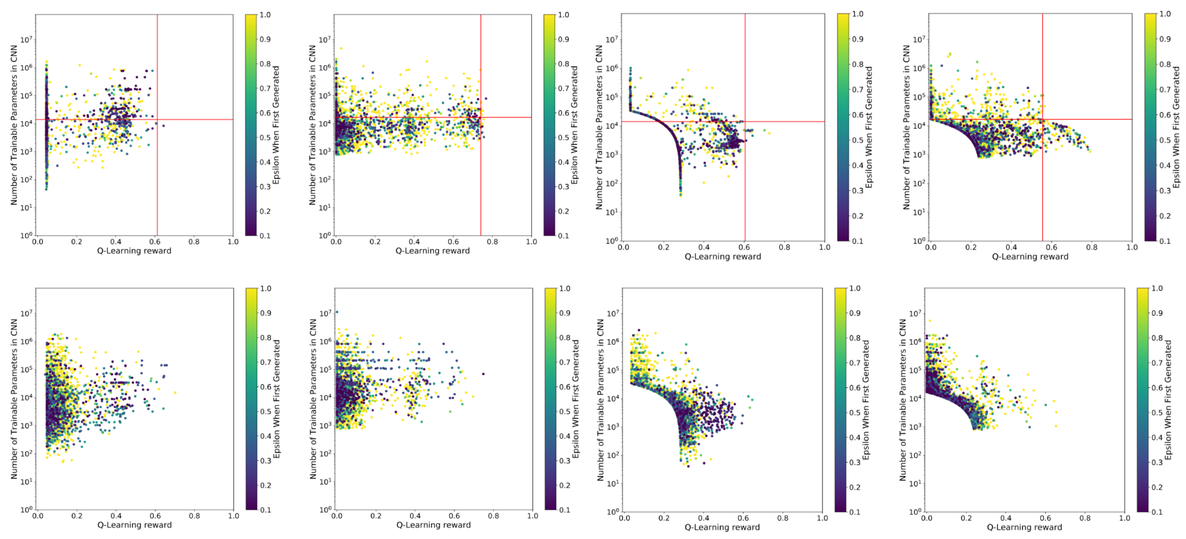
$$GE'_{10} = \frac{128 - \min(GE_{10}, 128)}{128}$$

$$GE'_{50} = \frac{128 - \min(GE_{50}, 128)}{128}$$

$$p' = \frac{\max(0, p_{\max} - p)}{p_{\max}}$$

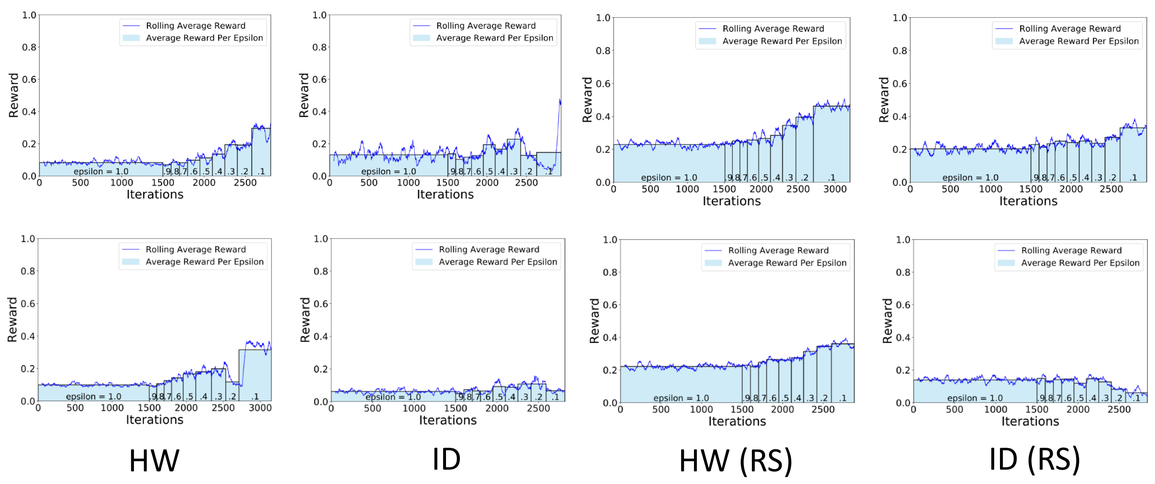
Results

Average rewards per epsilon



HW ID HW (RS) ID (RS)

Rolling average of the reward



HW ID HW (RS) ID (RS)

Trainable parameters & Guessing entropy

ASCAD Fixed Keys	HW Model			
	[ZBHV19]	[WPP20]	Best CNN	Best CNN (RS)
Trainable Parameters	14 235	1 336 753	8 480	5 566
$\overline{Q}_{t_{GE}}$	1 346	965	1 246	906

ASCAD Random Keys	HW Model			
	[PCP20]	[WPP20]	Best CNN	Best CNN (RS)
Trainable Parameters	N/A	1 314, 009	15 241	9 093
$\overline{Q}_{t_{GE}}$	470	496	911	1 264

ASCAD Fixed Keys	ID Model				
	[ZBHV19]	[WAGP20]	[WPP20]	Best CNN	Best CNN (RS)
Trainable Parameters	16 960	6 436	3 510 424	79 439	1 282
$\overline{Q}_{t_{GE}}$	191	≈ 200	155	202	242

ASCAD Random Keys	ID Model			
	[PCP20]	[WPP20]	Best CNN	Best CNN (RS)
Trainable Parameters	N/A	2 076 744	70 492	3 298
$\overline{Q}_{t_{GE}}$	105	1 568	490	1 018