

**“Classical” side-channel attacks**

```
Big Picture

Profilered Side-channel distinguisher
Template Attack
Stochastic Approach
Support Vector Machines [1]

Non-Profilered Side-channel distinguisher
Differential Power Analysis
Correlation Power Analysis
Mutual Information Analysis
Inter-class Information Analysis [2]
```

Open questions

- How to (fairly) compare side-channel distinguishers? [3]
- How to theoretically model side-channel attacks, e.g., with an information theoretic model?
- How to precisely (effectively) model the arising side-channel leakage from the device?

Web side-channel scenarios

```
```

“Modern” Web Side-channel attacks

```

```

Contact annelie.heuser@telecom-paristech.fr

Web http://perso.telecom-paristech.fr/~heuser/