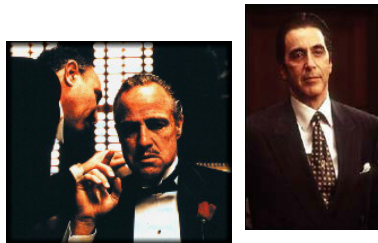


Are software and hardware counter-measures winning the war against side-channel leakage?

François Koeune

What do we mean by winning?

- Industry wins: manages to produce an invincible smart card



What do we mean by winning?

- Industry wins: manages to produce an invincible smart card
- Pirates win: smart cards disappear from the market
- As always, security is a trade-off

Countermeasures win

If we can say

- Choose a resistance level, depending on
 - Value of your data
 - Power of your adversary: knowledge, resources, ...
- We will be able to provide you, **for a given cost**, with a device having that resistance level

Evaluating resistance level

- Adversary's power
 - Resources
 - Skills
- Attacks' power
 - State-of-the-art
- Countermeasures' effectiveness

Can open literature provide us
with means of evaluating attacks
and designing sound
countermeasures?

What can we find in public literature ?

- Attacks
- Countermeasures
 - Software
 - Hardware
- Theoretical models

Can theoretical models provide a solution?

- *As a first approximation, we ignore coupling effects and create a linear model, i.e., we assume that the power consumption function of the chip is simply the sum of the power consumption functions of all the events that take place ... [CJRR99]*
- *Small couplings [...] provide a rich source of compromising emanations. [...] Exploiting [these] emanations can be much more effective than trying to work with direct emanations [AARR02]*