Internship Proposal:
“Comparison of side-channel attacks”

Superviser: Sylvain Guilley
Département Communication et Électronique
Institut TELECOM / TELECOM ParisTech
46, rue Barrault – 75634 Paris Cedex 13
Tél.: (33) 1 45 81 77 24
Fax: (33) 1 45 80 40 36

State of the Art
Any electronic device (smartcard, remote car key, smartphone, etc.) embeds cryptography to prevent from being badly used by unintended users (attackers). One classical scenario consists in collecting a physical emanation leaked by the device, such as the time it takes to respond to requests, or the magnetic field it radiates. These signals provide a noisy and non-injective information about the internal variables, that are sensitive in that they depend on cryptographic keys. Standard test platforms exist “off-the-shelf” to collect the side-channel signals.

Problem
However, the retrieval of the keys from those signals is complicated. This research field is very active, and many attacks have shown up. The usual methodology consists in defining a distinguisher that could differentiate the correct key from incorrect guesses (operating byte by byte, for instance). When few or no information is available from the attacked platform, so-called “generic” distinguishers are needed. They are usually statistical metrics that observe the empirical distributions, such as MIA (Mutual Information Analysis), IIA (Inter-class Information Analysis), (I)KSA (Inter-class Kolmogorov-Smirnov Analysis) or CEA (Cross-Entropy Analysis). There is no formal theory to decide which distinguisher is the best; therefore, tests should be performed to derive general rules of adequation between a leaking device and the corresponding adapted distinguisher.

Organization
During this training period, the student will:

1. Get acquainted with side-channel traces collection and attacks,
2. Participate to the DPA contest v4 (organized and hosted at TELECOM-ParisTech), where traces are freely available from a database,
3. Compare MIA, IIA, (I)KSA and CEA between themselves and to other attacks already submitted,
4. Infer some rules of thumb to associate to a leakage characteristic with the best matching distinguisher.

Miscellaneous information

- **Theme**: sécurité/cryptologie
- **Laboratory**: TELECOM-ParisTech, 75013 PARIS
- **Research group**: SEN
- **Internship director**: sylvain.guille@TELECOM-ParisTech.fr
- **Responsible of the laboratory**: jean-luc.danger@TELECOM-ParisTech.fr
- This work is funded by the Google company, via the fellowship in privacy won by my PhD student Annelie Heuser