MINES
Saint-Étienne

AGENCE NATIONALE DE LA RECHERCHE
ANR

Postdoctoral Position

ANR Project PANDORE (Protection Against New kinD Of Reverse Engineering)

Subject: Spatio-temporal and multiscale image analysis of secure circuits

Location: Ecole Nationale Supérieure des Mines, Saint-Etienne, FRANCE

Duration: The position is available now and is funded for 18 months.

Salary: The recipient will receive a net (free of taxes) income around 2000 euros.

Required qualifications:

- Candidates should have a Ph.D. (or equivalent qualification) in applied mathematics or computer sciences, focusing on image processing and analysis or very closely related areas;
- Programming skills with Matlab and C/C++;
- A good level of written and spoken English.

Application procedure:

- Candidates should send an application letter with a PDF detailed CV and diploma photocopies, together with a list of publications, a PDF copy of their PhD thesis and at least two reference letters.
  Documents should be sent at Johan DEBAYLE: debayle@emse.fr

Information:

For more information, please contact:

Dr. Johan DEBAYLE
Ecole Nationale Supérieure des Mines - 158 cours Fauriel - 42023 Saint-Etienne, FRANCE
Email: debayle@emse.fr ; Phone number: (+33) (0)477420219 ; Homepage: http://www.mines-stetienne.fr/~debayle/

Context: Disastrous societal, social and economic consequences could show up if confidential data stored in secure circuits (NFC circuits, smart meters, banking cards…) become easily accessible by badly intentioned people. Several techniques, based on the observation, the perturbation or the inspection of such devices have already been used for attacking those devices. These attacks are generally realized with a two-step approach. The first one consists in identifying critical functions within a transaction (time domain) and the position of these functions in the circuit (spatial domain). During the second phase, the attacker gather its mean over these functions, for instance to extract secrets or deactivate protections. The first phase, also called reverse-engineering phase, is critical for the attacker as it determines the efficiency to extract the secret in the second phase.

Currently, reverse-engineering techniques are mostly based on the circuit visual inspection. Recently, more affordable techniques that also give timing information have been proposed and validated on test circuits. In the near future, the combination of several techniques, giving various spatial and timing resolutions, would lead to a multi-scale reverse-engineering. This approach will decrease the cost and the time of the reverse engineering step, significantly reducing the component security. This is absolutely urgent that secure circuits manufacturers propose and validate efficient hardware and software protection against the multi-scale reverse-engineering techniques with a cost compatible with the targeted products.

PANDORE's consortium will include a small company, a major company and two academic laboratories. Each partner has recognized expertise in secure circuit and product design and has access to state of the art equipments to validate the proposed solutions. PANDORE project objective is dual. It has to:
- Quantify precisely the threat linked to multi-scale reverse engineering techniques
- Analyze the efficiency according to this new threat of current protections against reverse engineering and if necessary to purpose new protections

Tasks description: The selected approach to reach the first goal will consist in setting up multi-scale reverse engineering techniques that seem for us the most promising. With this in mind, we will improve the existing techniques by choosing probes and sensors more successful but also by proposing signal and image processing algorithms perfectly adapted. Data fusion (images and signals) obtained at different resolutions will be necessary to set-up the reverse engineering that we propose. This is a technical challenge already identified that will have to be unlocked. Indeed the data fusion needs specific registration methods in order to make some correspondences of geometrical and/or radiometric pattern at different spatial and temporal scales. Finally, to estimate the threat of these new techniques, it will be necessary to set them up over prototype and commercial circuits and then to quantify the obtained gain in spatial and temporal resolution.