



Secure-IC – Postes à pourvoir

Ingénieur 1a : BCDL

Réf. à rappeler : SIC-010

contact : hassan.triqui@secure-ic.com

Contexte

- Secure-IC est une start-up centrée sur la sécurisation des circuits logiques intégrés dédiés à la cryptographie.

Profil

- Ingénieur, conception d'architecture, intégration SoC
- Connaissance Outil requis (Environnement de travail) : CAO conception logique intégrée
- Expérience professionnelle antérieure souhaité : (1 à 3 ans d'expérience)
- Grande école d'ingénieurs, 3ème cycle universitaire souhaitable (**TELECOM ParisTech, ENSTA, Orsay, Ensea, ISEN**)

Mission

- Etude de conception d'architecture, intégration SoC
- Début : **avril 2010**

Description du poste et du contexte opérationnel

Cet ingénieur sera un concepteur, qui aura pour mission de sélectionner l'architecture d'un module de chiffrement AES, et de mettre en place un flot de conception visant à projeter ce bloc d'une description non protégée (référence) en une description en logique BCDL (à évaluer). Différentes options de performance seront étudiées : priorité à la vitesse, ou à la surface, dans le cas d'une cible FPGA ou ASIC.

Sa mission sera ensuite d'intégrer les deux blocs (référence et BCDL) dans un système sur puce (SoC), probablement dérivé d'EveSoC, en vue de leur évaluation sur banc d'injection de fautes (overclocking, glitch, laser) et d'attaque en observation (analyse en courant et EMA).



Secure-IC – Postes à pourvoir

Ingénieur 1b : BCDL

Réf. à rappeler : SIC-015

contact : hassan.triqui@secure-ic.com

Contexte

- Secure-IC est une start-up centrée sur la sécurisation des circuits logiques intégrés dédiés à la cryptographie.

Profil

- Ingénieur en électronique, connaissance en logique intégrée
- Notion de cryptographie
- Expérience professionnelle antérieure souhaité : (1 à 3 ans d'expérience)
- Grande école d'ingénieurs, 3ème cycle universitaire souhaitable (**TELECOM ParisTech, ENSTA, Orsay, Ensea, ISEN**)

Mission

- Evaluation de sécurité de logique intégrée, développement d'attaques sur logique intégrée
- Début : **avril 2010**

Description du poste et du contexte opérationnel

Le profil de cet ingénieur sera à dominante électronique avec des notions de cryptographie. Sa mission consistera en la caractérisation sécuritaire puis en l'évaluation des implémentations d'AES étudiées. En plus du travail d'acquisition de mesures de canaux cachés, cet ingénieur développera également des attaques spécifiques pour la logique DPL.

En logique DPL, contrairement aux logiques classiques non protégées, il y a un certain nombre d'hypothèses qui ne tiennent plus. Aussi, cet ingénieur interagira fortement avec l'ingénieur chargé de l'intégration SoC durant la phase de mise en place des attaques, pour adapter le banc aux vulnérabilités latentes de BCDL, comme la possible capacité de dissymétriser légèrement l'équilibrage du DPL par un positionnement particulier d'une micro-antenne magnétique en champ proche.



Secure-IC – Postes à pourvoir

Ingénieur 2 : REI S2PC

Réf. à rappeler : SIC-020

contact : hassan.triqui@secure-ic.com

Contexte

- Secure-IC est une start-up centrée sur la sécurisation des circuits logiques intégrés dédiés à la cryptographie.

Profil

- Ingénieur de recherche, conception logique intégrée, preuve formelle de sécurité
- Connaissance Outil requis (Environnement de travail) : Formality ou COQ
- Expérience professionnelle antérieure souhaité : (0 à 3 ans d'expérience)
- Grande école d'ingénieurs, 3ème cycle universitaire souhaitable (**Thèse de doctorat ou TELECOM ParisTech, TELECOM Bretagne, ENSTA, Orsay, UVSQ**)

Mission

- Etude et établissement de preuve de conformité et de propriété de sécurité
- Début : **avril 2010**

Description du poste et du contexte opérationnel

Le profil recherché est celui d'un jeune chercheur ayant déjà de l'expérience avec l'un ou l'autre des outils **Formality** ou **Coq**, ainsi qu'une bonne connaissance des méthodes formelles en général.

La mission de cet ingénieur de recherche est de réaliser d'une part une preuve de conformité et d'autre part une preuve de certaines propriétés de sécurité sur un circuit sécurisé.

L'objet étudié est une description de circuit, appelée "netlist", qui consiste en un graphe orienté de portes booléennes. En plus de réaliser une fonctionnalité déterminée, le graphe présente la particularité d'être redondant, afin de satisfaire à des besoins de sécurité. Par exemple, une topologie sciemment redondante du graphe combinée avec une fonction idoine des nœuds peut garantir des chemins de même longueur pour toutes les d'exécutions. Cette caractéristique confère à la netlist une robustesse par rapport à des attaques dites sur "canaux auxiliaires" qui savent exploiter les différences de longueurs de chemin.

Le travail commencera par une analyse des problèmes à résoudre (conformité, sécurité) exprimés en langage humain, puis par leur formalisation. Cette étape conduira à des choix quant à la méthodologie la plus adéquate pour résoudre les problèmes. Il s'agira notamment de partitionner les preuves en trois catégories :

1. celles qui peuvent être réalisées mathématiquement, sans l'aide d'aucun outil, étant donné les spécificités des techniques de contre-mesure (propriétés topologiques de la netlist),
2. celles qui nécessitent le concours d'un outil, qui peut être un outil commercial, et enfin,
3. celles qui nécessitent le recours à un outil ad hoc, qu'il s'agira alors de développer et de coder sur mesure en interne.

Au cours de sa mission, ce chercheur sera en charge d'animer un séminaire de rencontre de différents acteurs du monde académique étudiant des méthodes formelles, dans le but de les sensibiliser au problème de la sécurisation des composants cryptographiques et de voir auprès d'eux si des synergies peuvent être dégagées pour de futures collaborations. L'objet de cette série de séminaires sera très clairement de constituer un réseau d'acteurs prêts à s'associer pour de futurs projets ayant trait à la preuve de correction des implémentations cryptographiques.



Secure-IC – Postes à pourvoir

Ingénieur 3 : Chef du projet Smart-SIC+

Réf. à rappeler : SIC-030

contact : hassan.triqui@secure-ic.com

Contexte

- Secure-IC est une start-up centrée sur la sécurisation des circuits logiques intégrés dédié à la cryptographie.

Profil

- Chef de projet, ingénieur en filière FPGA ou ASIC, sensibilisé à la sécurité
- Connaissance Outil requis : Conception FPGA Xilinx, gestion de projet
- Expérience professionnelle antérieure souhaité : **(5 ans minimum)**
- Grande école d'ingénieurs ou 3ème cycle universitaire (**Ecole polytechnique, TELECOM ParisTech, TELECOM Bretagne, Sup Elec, ESIEE, ENSEA, ISEN, Orsay**)

Mission

- Chef de projet carte à puce
- Début : **avril 2010**

Description du poste et du contexte opérationnel

Le projet Smart-SIC+ consiste en la mise au point d'une carte à puce de nouvelle génération, qui soit d'un niveau de sécurité supérieur à l'existant, de par la nature "avancée" de ses contre-mesures et leur caractère "formellement prouvé".

Le chef de projet Smart-SIC+ est un ingénieur sénior, dont la mission sera de :

- spécifier l'architecture haut-niveau du système sur puce (SoC) constituant la carte à puce, sur la base de la famille de composants développés et maintenus par TELECOM-ParisTech,
- intégrer dans le SoC des briques cryptographiques robustes de technologie hétérogène (comme de la logique à deux rails) provenant d'autres programmes de recherche de Secure-IC,
- auditionner, sélectionner et encadrer des ingénieurs embauchés afin de mener à bien la conception, l'émulation, le tape-out et l'évaluation de Smart-SIC+.

Le profil du chef de projet sera davantage celui d'un ingénieur ayant une expérience dans le développement de systèmes (matériel ou de logiciel) complexes, doté une bonne maîtrise de la gestion de projets et du respect des contraintes (humaines, temporelles, budgétaires) et disposant d'un bagage suffisant pour suivre et guider efficacement l'avancement des développements.

En plus de cet encadrement, le chef de projet assurera la promotion du produit Smart-SIC+ à des partenaires ou des prospects ; à cette fin, il participera à des salons et présentera Smart-SIC+ à des évaluations et à des concours.

Enfin, le chef de projet Smart-SIC+ assurera une veille technologique par rapport à l'offre concurrente et au besoin des clients, notamment du domaine très exigeant des cartes à puces évaluées formellement.



Secure-IC – Postes à pourvoir

Ingénieur 4 : Test et Evaluation de Smart-SIC+.

Réf. à rappeler : SIC-040

contact : hassan.triqui@secure-ic.com

Contexte

- Secure-IC est une start-up centrée sur la sécurisation des circuits logiques intégrés dédié à la cryptographie.

Profil

- Ingénieur test et validation, Technicien Supérieur en conception logique intégrée
- Connaissance Outil requis : Oscilloscope numérique, Outils de conception FPGA
- Expérience professionnelle antérieure souhaité : **(0 à 5 ans)**
- Ecole d'ingénieurs, DUT avec expérience

Mission

- Assistance au développement FPGA et ASIC, développement de tests et validations
- Début : **avril 2010**

Description du poste et du contexte opérationnel

La mission consiste à assister le développement et la validation d'une carte à puce de nouvelle génération, nommée Smart-SIC+.

L'ingénieur sera impliqué dès la phase de spécification du circuit, soit pour contribuer à la conception de certains blocs, soit pour réaliser des tests unitaires. Puis, quand un prototype sera fonctionnel (Q2 2010), cet ingénieur sera responsable du test de la carte à puce émulée sur FPGA.

En liaison avec les équipes de développement d'IP matérielles sécurisées, il contribuera à leur intégration dans le prototype Smart-SIC+. Ensuite, il gèrera les évolutions du projet, versionné sur un système de développement collaboratif de type "subversion". Ce système, administré par l'ingénieur, permettra entre autres d'échanger des données avec les équipes de TELECOM ParisTech et d'éviter les régressions.

Une ramification du projet consistera notamment en son portage sur cible ASIC. À ce titre, l'ingénieur acquerra un double savoir-faire en conception avec les familles Stratix et l'outil Quartus d'Altera (produit final FPGA) et avec la technologie 45 nanomètres de STMicroelectronics et les outils Cadence (produit final ASIC).

Enfin, l'ingénieur aidera à réaliser les attaques en pénétration sur le composant, dans son avatar FPGA ou ASIC, dans l'optique d'évaluer sa résistance par rapport aux attaques en injection de faute et en observation. Une expérience préalable en certification (FIPS 140-3 ou Critères Communs) est un atout dans ce poste.

La mission requiert de bonnes connaissances et une affinité pour l'électronique et la conception FPGA en collaboration avec le chef de projet.