Proposition de recherche doctorale

Insertion automatique de contre-mesures dans des circuits de sécurité.

Mots clés :

- **Directeur de thèse** : JEAN-LUC DANGER
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire Traitement et Communication de l'Information
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Les protections dans les circuits intégrés sensibles sont souvent ajoutées à la main après la conception. Il en résulte potentiellement différents problèmes : la protection peut être simplement mal codée, et donc impacter la fonctionnalité ou bien ne pas protéger comme prévu. Ou encore, la mise en place de la contremesure peut-être très inefficace. Pour toutes ces raisons, il peut être souhaitable de mettre en place des contre-mesures automatiquement par un outil d'aide à la conception. Même si les portions de codes sensibles sont fréquemment écrites à la main, différentes expériences en ce sens ont déjà été réalisées. Par exemple, dans le domaine des portes logiques, on peut citer {DBLP:journals/tcad/TiriV06} , {ghavamipatmos07}, {DBLP:conf/dac/BayrakRBSI11} et au niveau d'un code logiciel {DBLP:conf/ches/MossOPT12}. Le travail démarrera par une revue de l'état de l'art des attaques, en vue de les classifier. Ensuite, un état de l'art similaire sera réalisé sur les contre-mesures. Un premier résultat sera de formaliser attaques et contre-mesures, dans l'optique de vérifier automatiquement quelles attaques sont contrées par quelles contre-mesures. Dans un second temps, deux contre-mesures seront étudiées plus en détail : -* une qui porte sur la résistance aux attaques passives (exploitation discrète d'un canal caché), et -* une autre qui porte sur la résistance aux attaques actives (analyse de résultats fautés pour en déduire les secrets). Puis, l'une d'entre elle sera implémentée. Sur la base de sa spécification formelle, on en extraira le nombre minimal de tests expérimentaux à réaliser sur valider les hypothèses de bon fonctionnement de la contre-mesure. Ensuite, la contre-mesure sera effectivement insérée automatiquement dans un flot de conception qui utilise les outils automatiques de conception assistée par ordinateur. Enfin, une évaluation sera réalisée : il est en effet important de faire cet exercice pour démontrer que même une contre-mesure abordée sous l'angle formel peut être efficace en pratique. Cet étape est essentielle pour motiver l'intérêt et l'utilité des méthodes formelles.

Résumé du projet de recherche (Langue 2)

Même si quelques preuves de concept ont été démontrées dans l'état de l'art, il reste de nombreux points importants à traiter. Il s'agit de définir des contre-mesures raisonnables, {i.e.} -* pas trop exigeantes ({e.g.} aucun programme utile ne pourra être écrit si l'on interdit l'existence ou l'utilisation de secrets), -* ni trop spécifiques, c'est-à-dire spécialisées pour une vulnérabilité donnée (auquel cas leur utilité sera remise en cause par un attaquant qui cible une partie non modélisée du système). Ensuite, il faut identifier le niveau d'insertion des contremesures : -* Si elles sont insérées trop haut, il sera peut-être difficile de vérifier que les contre-mesures restent efficaces malgré les transformations opérées par la chaîne de compilation ; -* Si elles sont insérées trop bas, elles auront un surcoût élevé. % peut-être trop grand. Enfin, il serait envisageable de spécifier des insertions de contre-mesures qui peuvent être optimisées, sans briser leur principe de fonctionnement.

Informations complémentaires (Langue 2)

{DBLP:conf/dac/BayrakRBSI11} Ali Galip Bayrak, Francesco Regazzoni, Philip Brisk, Francois-Xavier Standaert, and Paolo Ienne. A first step towards automatic application of power analysis countermeasures. In Leon Stok, Nikil D. Dutt, and Soha Hassoun, editors, DAC, pages 230–235. ACM, 2011. {ghavamipatmos07} Behnam Ghavami and Hossein Pedram. An Automatic Design Flow for Implementation of Side Channel Attacks Resistant Crypto-Chips. In Springer, editor, Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation, 17th International Workshop, PATMOS, volume 4644 of LNCS, pages 330–339, September 3-5 2007. Gothenburg, Sweden. {DBLP:conf/ches/MossOPT12} Andrew Moss, Elisabeth Oswald, Dan Page, and Michael Tunstall. Compiler Assisted Masking. In Emmanuel Prouff and Patrick Schaumont, editors, CHES, volume 7428 of Lecture Notes in Computer Science, pages 58–75. Springer, 2012. {DBLP:journals/tcad/TiriV06} Kris Tiri and Ingrid Verbauwhede. A digital design flow for secure integrated circuits. IEEE Trans. on CAD of Integrated Circuits and Systems, 25(7) :1197–1208, 2006.