CNRS, nouvelle technologie pour sÃ©curiser les systÃ¨mes et circuits intÃ©grÃ©s
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 3/4/2009 15:00:00

Le LIRMM, laboratoire dâ□informatique, de robotique et de microÃ©lectronique de Montpellier (CNRS/UniversitÃ© Montpellier 2) vient de mettre au point une **nouvelle technologie capable de rÃ©duire lors de transactions Ã©lectroniques jusqu'Ã 95 % les fuites d'informations** des circuits intÃ©grÃ©s par rapport Ã des circuits logiques classiques.
Celle-ci fait actuellement l'objet dâ□une collaboration entre le LIRMM et la sociÃ©tÃ© PSI Electronics, sociÃ©tÃ© spÃ©cialisÃ©e dans la conception de circuits et systÃ¨mes intÃ©grÃ©s, dans la perspective dâ□un transfert de technologie.

Â

Â

Les attaques matÃ©rielles sâ□Ã©tant gÃ©nÃ©ralisÃ©es, la cryptologie est dÃ©sormais devenue incontournable dans la conception des systÃ¨mes numÃ©riques qui supplantent le papier comme supports de l'information. Ces attaques touchent les composants matÃ©riels oÃ¹ vont sâ□exÃ©cuter les logiciels (puces, microprocesseurs...).

Elles sont reconnues comme les plus dangereuses car elles permettent d'obtenir Ã moindre frais et avec un faible niveau de compÃ©tences les clefs des algorithmes de chiffrement, comme ceux qu'utilisent nos cartes Ã puce.

La nouvelle logique Â«STTLÂ» (**Secure Triple Track Logic**) dÃ©veloppÃ©e par le LIRMM est trÃ¨s efficace contre les attaques et piratages matÃ©riels des circuits intÃ©grÃ©s prÃ©sents dans les cartes Ã puces, cartes sim, processeurs... nÃ©cessitant Ã la fois authentification et confidentialitÃ© des informations.

Â

Elle permet de rÃ©duire jusqu'Ã 95 % les fuites d'informations des circuits intÃ©grÃ©s par rapport Ã des circuits logiques classiques. Ceci grÃ¢ce Ã ses particularitÃ©s : elle possÃ¨de un temps de calcul constant et maintient rÃ©guliÃ¨re la consommation Ã©lectrique du circuit, deux failles rÃ©currentes lors dâ□□attaques matÃ©rielles et jusque lÃ non maÃ®trisÃ©es.

Le LIRMM et PSI Electronics travaillent en partenariat pour transfÃ©rer vers l'industrie cette nouvelle technologie issue du laboratoire de recherche. Elle sera utilisÃ©e dans la conception de circuits et systÃ¨mes intÃ©grÃ©s.

La sociÃ©tÃ© PSI, basÃ©e dans la rÃ©gion dâ□□Aix-en-Provence a dÃ©jÃ dÃ©veloppÃ© une premiÃ¨re bibliothÃ¨que de composants (4) qui devrait permettre une rapide validation Ã l'Ã©chelle industrielle, complÃ©tant ainsi sa compÃ©tence particuliÃ¨re en conception de circuits intÃ©grÃ©s sÃ©curisÃ©s.

Ces travaux, dÃ©veloppÃ©s initialement au LIRMM, se poursuivent depuis deux ans dans le cadre du projet CALISSON ("CAractÃ©risation, modÃ©LIsation et SpÃ©cifications SÃ©curitaires de circuits prOtotypes iNtÃ©grÃ©s"), financÃ© par le ministÃ¨re de l'Industrie et labellisÃ© par le PÃ´le de CompÃ©titivitÃ© mondial SCS (6), en juin 2006.

Outre la sociÃ©tÃ© PSI, CALISSON a Ã©galement pour partenaires industriels STMicroÃ©lectronics, Gemalto (fabricant de cartes bancaires), Atmel (fabricant de composants de circuits intÃ©grÃ©s), mais aussi acadÃ©miques comme Parisâ□□Tech, lâ□□Ã©cole des Mines de Saint Etienne (ENSMSE) et le CEA.