Cryptography Research annonce l'intégration de SASEBO-G à sa plateforme DPA Workstation(TM)

San Francisco (Etats-Unis), le 23 juin 2009 – Cryptography Research, Inc. (CRI) annonce aujourd'hui l'intégration de l'outil SASEBO-G (Side-Channel Attacks Standard Evaluation Board, version révisée) à sa plateforme DPA Workstation(TM), pour permettre de tester des images FPGA contre les attaques matérielles par canaux cachés (attaques dites « side-channel »), comme les attaques par analyse simple (SPA) ou différenciée (DPA) de la consommation de charge électrique.

La dernière version du logiciel DPA Workstation (v 6.16) offre la possibilité de tester les FPGAs en utilisant l'outil SASEBO-G développé par l'AIST (National Institute of Advanced Industrial Science and Technology) au Japon. Cette version propose également des outils améliorés de visualisation pour interpréter et manipuler les courbes d'analyse du courant.

Le SASEBO-G propose une plateforme optimisée pour réaliser des analyses de charges sur les images FPGA Xilinx. Le logiciel de collecte des données et d'analyse développé par CRI inclut la fonction directe I/O, ainsi que des capacités de collecte de données dans la plateforme SASEBO-G. M. Akashi Satoh, directeur du projet SASEBO au sein de l'AIST, indique : « Nous sommes ravis de travailler avec Cryptography Research et d'offrir une nouvelle capacité d'évaluation de modules cryptographiques sophistiqués face à des attaques side-channel. »

La plateforme DPA Workstation est une pionnière dans le domaine de l'analyse des attaques side-channel, et permet de tester une grande quantité de dispositifs qui fonctionnent avec les principaux algorithmes cryptographiques, tels que DES, 3DES, AES, RSA, algorithmes à courbe elliptique, SHA, ainsi que des algorithmes développés en interne. « L'intégration de l'outil SASEBO-G dans notre plateforme DPA Workstation(TM) confirme l'engagement de CRI à proposer des outils d'évaluation à la pointe de la technologie pour protéger les dispositifs de terrain contre les analyses de différences de charge et autres attaques side-channel, » souligne Benjamin Jun, le vice-président Technologie de CRI.

A propos de SASEBO
Les outils SASEBO (Side channel Attack Standard Evaluation Boards) ont été développés par le Centre de Recherche en Sécurité de l'Information (Research Center for Information Security ou RCIS) de l'AIST (National Institute of Advanced Industrial Science and Technology- Japon), en collaboration avec l'université Tohoku, dans le cadre de projets de recherche sponsorisés par le Ministère de l'Economie, du Commerce et de l'Industrie du Japon (METI - Ministry of Economy, Trade and Industry) pour fournir une référence d'évaluation standard pour les modules cryptographiques.
Plus d'information sur : http://www.rcis.aist.go.jp/special/SASEBO/index-en.html

A propos de la plateforme DPA Workstation(TM)
La plateforme DPA Workstation(TM) de Cryptography Research est une plateforme puissante et flexible permettant de tester les analyses side-channel. Elle est utilisée partout dans le monde par de nombreuses sociétés et par des gouvernements. La plateforme DPA Workstation(TM) inclut le matériel, les logiciels et les instructions nécessaires pour réaliser des tests et des évaluations sophistiquées d'analyses de charge. Le code source est fourni en intégralité, ce qui permet de customiser la plateforme pour l'utilisation dans de nombreux environnements et avec de nombreux dispositifs.

A propos de Cryptography Research Inc.
Cryptography Research Inc. fournit des solutions technologiques qui permettent de résoudre des problèmes de sécurité complexes. En plus de l'audit des paramètres de sécurité et l'élaboration de réponses technologiques adaptées aux besoins de ses clients, Cryptography Research mène des recherches à long terme et vend des licences de sa

technologie dans des domaines variés dont la détection des falsifications, la protection des contenus, la sécurité des réseaux et des services financiers. Les systèmes de sécurité conçus par Cryptography Research protègent chaque année un volume de transactions de plus de 100 milliards de dollars dans les secteurs du sans-fil, des télécommunications, de la finance, de la télévision numérique et de l'Internet.
Pour plus d'information : http://www.cryptography.com