Mercredi 20 septembre 2017 à 10h à Gardanne en salle HS002.

« Sécurisation des algorithmes de couplages contre les attaques physiques »

Composition du jury proposé

M. Louis GOUBIN Univ. Versailles-Saint-Quentin-en-Yvelines, Directeur de thèse
M. Christophe CLAVIER, Université de Limoges - Rapporteur
M. Jean-Guillaume DUMAS, Université Grenoble Alpes - Rapporteur
M. Benoît GERARD, Direction Générale de l'Armement - Examinateur
M. Sylvain GUILLEY, TELECOM-ParisTech - Examinateur
Mme Vanessa VITSE,Université Grenoble Alpes - Examinatrice
M. Jacques J.A. FOURNIER, CEA-LETI - Encadrant
Mme Nadia EL MRABET, MINES Saint-Étienne - Encadrante

Résumé de la thèse de Damien Jauvart

Cette thèse est consacrée à l'étude de la sécurité physique des algorithmes de couplage. Les algorithmes de couplage sont depuis une dizaine d'années utilisés à des fins cryptographiques. D'une part, les systèmes d'information évoluent, et de nouveaux besoins de sécurité naissent.

Les couplages permettent des protocoles innovants, tels que le chiffrement basé sur l'identité, les attributs et encore l'échange triparti en un tour. D'autre part, l'implémentation des algorithmes de couplages est devenue efficace, elle permet ainsi d'intégrer des solutions cryptographiques à base de couplage dans les systèmes embarqués. Cette nouvelle facette des couplages va être étudiée ici.

En effet, l'implémentation d'algorithmes dédiés à la cryptographie sur les systèmes embarqués soulève une nouvelle problématique : la sécurité de l'implémentation des couplages face aux attaques physiques. Les attaques par canaux auxiliaires, dites passives, contre les algorithmes de cryptographie sont connues depuis bientôt une dizaine d'années.

Nous proposons des études pour valider l'efficacité des attaques, à la fois en pratique et avec des atouts théoriques. L'attaque de l'état de l'art a ainsi été optimisée d'un facteur dix en termes de nombres de traces. Nous proposons aussi une attaque horizontale, qui nous a permis d'attaquer le couplage twisted Ate en une seule trace. Par ailleurs, les contre-mesures n'ont été que peu étudiées. Nous complétons cette partie manquante de la littérature.

Nous proposons de nouveaux modèles d'attaques sur la contre-mesure de randomisation des coordonnées. L'attaque en collision proposée permet ainsi de donner une expertise de la contre-mesure ciblée.

Nous tirons de cette expertise une implémentation élaborée de la contre-mesure. Nous appliquons la contre-mesure, puis nous donnons son implémentation en cherchant les meilleurs paramètres d'efficacité.

Mots-clés : Cryptographie, Couplages, Attaques par canaux auxiliaires, Contre-mesures