Application BASTRI

Fiches Equipes

CASCADE (SR0095XR)

Conception et Analyse de Systèmes pour la Confidentialité et l'Authentification de Données et d'Entitées
CASCADE

Statut: Décision signée

Responsable : Phong-quang Nguyen

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2024" : A4. Sécurité et confidentialité , A4.3. Cryptographie , A4.3.1. Cryptographie à clé publique , A4.3.2. Cryptographie à clé secrète , A4.3.3. Protocoles cryptographiques , A4.3.4. Cryptographie quantique , A4.8. Technologies pour la protection de la vie privée , A7. Informatique théorique , A7.1.4. Algorithmique quantique , A8.5. Théorie des nombres , A8.9. Evaluation de performances , A8.10. Arithmétique des ordinateurs

Mots-clés de "B - Autres sciences et domaines d'application - 2024" : B6.4. Internet des objets , B9.5.1. Informatique , B9.10. Confidentialité, vie privée

Domaine : Algorithmique, programmation, logiciels et architectures
Thème : Algorithmique, calcul formel et cryptologie

Période : 01/07/2008 -> 31/12/2028
Dates d'évaluation : 24/03/2011 , 17/03/2015 , 19/03/2019 ,

Etablissement(s) de rattachement : CNRS, ENS PSL
Laboratoire(s) partenaire(s) : DI-ENS (UMR8548)

CRI : Centre Inria de Paris
Localisation : Ecole Normale supérieure Paris
Code structure Inria : 021085-1

Numéro RNSR : 200818333X
N° de structure Inria: SR0095XR

Présentation

La cryptographie, ou science du secret, a pour objectif de sécuriser les supports et les échanges de données numériques. Pour cela, deux activités s'opposent : celle qui consiste à construire des systèmes permettant d'atteindre cet objectif, et l'attaque qui tente de mettre en défaut certaines propriétés de sécurité. L'équipe-projet CASCADE étudie un spectre très large de la cryptographie : la construction de primitives et de protocoles cryptographiques, avec leur analyse de sécurité, et le cas échéant l'attaque, aussi bien aux niveaux mathématique et algorithmique, qu'au niveau de la mise en oeuvre effective, en exploitant les failles d'implémentation ou les fuites d'information liées au matériel.

Axes de recherche

Les objectifs de sécurité les plus urgents à résoudre, et qui constituent nos priorités, sont la protection de la vie privée et la protection des contenus. Avec ce monde du tout-numérique, des profils d'individus peuvent aisément être constitués, les contenus (flux audios, vidéos, etc) peuvent également être diffusés et dupliqués. La cryptographie permet de limiter les abus, et de contrôler les informations collectées.

D'un point de vue constructif, une des compétences, et spécialité, de l'équipe-projet CASCADE est la "sécurité prouvable". La construction d'un système cryptographique ne suffit pas à garantir la sécurité souhaitée, encore faut-il le prouver. Pour cela, il est nécessaire, dans un premier temps, de caractériser les notions de sécurité requises, et donc de modéliser cela sous un formalisme adéquat. Ainsi, on prouve qu'attaquer l'une de ces notions revient obligatoirement pour l'attaquant à mettre à mal une hypothèse algorithmique reconnue difficile de tous.

Cette "sécurité prouvée" ne réduit pas l'activité des cryptanalystes à néant, car des failles peuvent se présenter à plusieurs niveaux : d'un point de vue mathématique, en remettant en question l'hypothèse algorithmique sous-jacente; au niveau protocole, en contournant le modèle de sécurité; au niveau implémentation, en pointant des erreurs de programmation ou de mise en oeuvre effective. Un biais d'attaque désormais classique est l'exploitation des

Contact

- **Responsable :** Phong-quang Nguyen
- **Tél :** 01.44.32.20.34
- **Secrétariat Tél :** 01.44.32.20.34

En savoir plus

- Site de l'équipe
- Site sur inria.fr
- Site du responsable
- Derniers Rapports d'Activité : 2016 , 2017 , 2018 , 2019 , 2020 , 2021 , 2022 , 2023

Documents sur la structure

- Intranet
- Privés

Décisions

- 6234 (11/07/2008) : création
- 8337 (19/01/2012) : prolongation
- 11315 (14/12/2015) : prolongation
- 14024 (16/12/2019) : prolongation
- 14349 (25/06/2020) : création
- 16661 (11/12/2023) : prolongation
- 17000 (26/04/2024) : prolongation
- 17069 (28/05/2024) : cessation du responsable
- 17070 (28/05/2024) : nomination responsable
- 17533 (06/12/2024) : prolongation

Localisation

- **Adresse postale :** École Normale supérieure 45 rue d'Ulm 75005 Paris France
- **Coordonnées GPS :** 48.841898, 2.345021

fuites d'information au niveau physique (canaux cachés), tels la consommation électrique ou le rayonnement électro-magnétique.

Relations industrielles et internationales