

# Application BASTRI

## Fiches Equipes

### PESTO (SR0758TR)

Techniques de Preuves pour les Protocoles de Sécurité  
PESTO (SR0729KR) □ PESTO

**Statut:** Décision signée

**Responsable :** Steve Kremer

**Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2023" :** A1.2.8. Sécurité des réseaux , A2.2.9. Sécurité par la compilation , A2.4. Méthodes formelles pour vérification, sureté, certification , A4.3.3. Protocoles cryptographiques , A4.5. Méthodes formelles pour la sécurité , A4.6. Authentification , A4.8. Technologies pour la protection de la vie privée , A7.1. Algorithmique , A7.2. Logique

**Mots-clés de "B - Autres sciences et domaines d'application - 2023" :** B6.3.2. Protocoles , B6.3.3. Gestion des réseaux , B6.3.4. Réseaux sociaux , B6.6. Systèmes embarqués , B9.10. Confidentialité, vie privée

**Domaine :** Algorithmique, programmation, logiciels et architectures  
**Thème :** Sécurité et confidentialité

**Période :** 01/11/2016 -> 31/12/2024  
**Dates d'évaluation :** 21/03/2019 ,

**Etablissement(s) de rattachement :** CNRS, U. DE LORRAINE  
**Laboratoire(s) partenaire(s) :** LORIA (UMR7503)

**CRI :** Centre Inria de l'Université de Lorraine  
**Localisation :** Centre Inria de l'Université de Lorraine  
**Code structure Inria :** 051105-1

**Numéro RNSR :** 201622052E  
**N° de structure Inria:** SR0758TR

### Présentation

L'objectif de l'équipe PESTO est de concevoir des modèles et techniques pour l'analyse et la conception assistée par ordinateur de protocoles de sécurité. Alors qu'historiquement les protocoles de sécurité visaient à protéger la confidentialité et l'authentification, la situation a changé. Les protocoles de vote électronique doivent garantir l'anonymat du votant, tout en garantissant la transparence du scrutin; les données sont transmises en utilisant des services web; les protocoles implantés dans les puces RFID et les téléphones portables doivent garantir qu'on ne puisse pas tracer les utilisateurs. À cause des logiciels malveillants de plus en plus répandus, les protocoles de sécurité utilisent de nouveaux mécanismes, tels que du hardware de confiance ou des authentifications multi-facteurs, afin de garantir des propriétés de sécurité et ceci même si la plateforme sur laquelle ces protocoles s'exécutent est compromise. Les techniques et outils existants sont cependant incapables d'analyser les propriétés de sécurité requises par ces nouveaux protocoles et de prendre en compte les nouveaux mécanismes déployés et modèles d'attaquants correspondants.

### Axes de recherche

- Formal methods for Cryptographic protocols
- Automated reasoning
- Electronic voting
- Privacy in social networks

### Relations industrielles et internationales

#### Contact

- **Responsable :** Steve Kremer
- **Tél :** 03.54.95.86.60
- **Secrétariat Tél :**

#### En savoir plus

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

#### Documents sur la structure

- Intranet
- Privés

#### Décisions

- **11873** (03/11/2016) : création
- **14026** (16/12/2019) : prolongation
- **16660** (11/12/2023) : prolongation
- **16999** (26/04/2024) : prolongation

#### Localisation

- **Adresse postale :** Centre Inria de l'Université de Lorraine, 615 rue du Jardin Botanique, 54600 Villers-lès-Nancy France
- **Coordonnées GPS :** 48.666, 6.157

