General information

Inria Rennes – Bretagne Atlantique

TAMIS team (*Threat Analysis and Mitigation for Information Security*)

Axel LEGAY (team leader); Olivier ZENDRA (me)

Axel.Legay@inria.fr ; Olivier.Zendra@inria.fr

+33 2 99 84 75 13; +33 3 54 95 84 07

Area of interest	Choose Y or N
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	Y
○ Ultra-lightweight cryptology and ultra-high-speed cryptographic algorithms including quantum cryptography	N
○ Physical cryptanalysis, including tampering, side channel, faults injection attacks, and security of tools for good software implementation and validation practices	Y
○ Authenticated encrypted token research for mobile payment solution	N
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	N
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	N
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	N

Competencies

- ***Organisation competencies:*** TAMIS works on formal methods, model checking, software engineering, program analysis, program transformation, memory management, hardware vulnerability analysis, malware analysis

- ***Organisation experience in European projects:*** +180 EU projects in FP6/FP7 for Inria (10 for TAMIS team)

- ***Environment:***
  - TAMIS cooperates with large groups (Cisco, Oberthur, Thales…) and SMEs (Secure-IC...).
  - Can give access to more via the Pôle D'excellence Cyber (Cyber Excellency Pole), in Brittany: large groups (Sopra, Cap Gemini, Orange, …), SMEs (Amossys, Diateam, ARX Défense & Sécurité, Tevalis...), academia (Inria, CNRS, Universities), MoD-related actors (DGA, defense schools...), etc.

Project idea(s)

- ***Describe your project idea(s):***
  1. (De)Obfuscation
  2. Dynamic program modification for protection

- ***List of the complementary skills you need for your consortium***
  1. Compiler vendors; Runtime vendors; Integrators (end users); Crypto analysts; Statisticians…
  2. Runtime vendors; Integrators (end users); Crypto analysts; Hackers / Malware “providers”; Defense authorities…