HORIZON 2020

LE PROGRAMME DE RECHERCHE ET
D'INNOVATION DE L'UNION EUROPÉENNE

Secure Societies
DS-06-2017 Cryptography

Paris September 5th, 2016

BROKERAGE SESSION

NOW: UNIVERSITÀ DEGLI STUDI DELL’AQUILA (LUIGI POMANTE)

NEXT: UNIVERSITY OF SURREY, UK (LIQUN CHEN)

General information

Università degli Studi dell'Aquila (ITALY)

- **Center of Excellence DEWS**

  Design Methodologies for Embedded controllers, Wireless interconnect and System-on-chip

  http://dews.univaq.it/

Dr. Luigi Pomante (Assistant Professor)

- **luigi.pomante@univaq.it**

Area of interest	**Choose Y or N**
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	N
○ Ultra-lightweight cryptology and ultra-high-speed cryptographic algorithms including quantum cryptography	Y
○ 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	Y
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	Y
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	N
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	Y

Competencies

- ***Design Methodologies for Networked Embedded Systems***
  - **W**ireless **S**ensor **N**etworks & **M**obile **A**d-hoc **NET**works

- *Relevant European Projects*
  - **SAFECOP (ECSEL-JU RIA-2015)**

    Safe Cooperating Cyber-Physical Systems using Wireless Communication
  - EMC2 (Artemis-JU 2013 AIPP)

    Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable RT environments
  - CRAFTERS (Artemis-JU 2011 ASP)

    ConstRaint and Application-driven Framework for Tailoring Embedded RT Systems
  - PRESTO project (Artemis-JU 2010 ASP)

    ImProvements of industrial Real Time Embedded SysTems develOpment process
  - **VISION (FP7 "Ideas" 2009 – ERC SGA)**

    Video-oriented UWB-based Intelligent Ubiquitous Sensing

- *Relevant skills*
  - **Lightweight Cryptography, Topology-based Key Management and Certification, and Intrusion Detection Systems for WSN and resource-constrained MANET**

NOW: UNIVERSITY OF SURREY, UK (LIQUN CHEN) NEXT: PRIM’X TECHNOLOGIES (PIERRE-JEAN LECA)

General information

University of Surrey, UK
Professor Liqun Chen
liqun.chen@surrey.ac.uk
+44 7814 752 577

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	Y
○ 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	Y
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	Y
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	Y
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	Y

Competencies

- *Surrey Centre for Cyber Security works together with*
  - 5G Innovation Centre, Surrey Space Centre, Centre for Digital Economy, Centre for Vision, Speech & Signal Processing, Department of Sociology, School of Law and School of Psychology
- *Involved in a number of EU FP7 projects, e.g.*
  - SENSEI (support for security, privacy and trust in sensor and actuator networks) 2007-2010
  - EXALTED (scalability and security for LTE networks) 2010-2013
  - Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures, 2012-2014
- *We can bring the skills of*
  - **Cryptography**, including functional encryption and quantum safe cryptography
  - **Hardware security**, such as crypto algorithms in Trusted Platform Modules
  - **Formal verification** for code, design and protocols
  - Security in **mobile communications** and **IoT**
  - **Privacy** enhancing technologies
  - **Trust**, identity management, authentication and access control
  - **Human-centred security**, e.g., e-voting and distributed ledger technology
  - **Digital forensics** and security engineering
  - **Cloud security** and **big data analysis**

NOW: PRIM’X TECHNOLOGIES (PIERRE-JEAN LECA)
NEXT: THALES UK, RESEARCH &TECHNOLOGY (ADRIAN WALLER)

General information

Prim'X Technologies

Pierre-Jean LECA

Pierre-jean.leca@primx.fr

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	Y
○ 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	Y
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	Y
○ Quantum key distribution	Y
○ Automated proof techniques for cryptographic protocols	N

Competencies

- *Software editor in CyberSecurity (encryption)*
- *Objectives:*
  - To protect data at rest in every location : laptops, servers, removable media, backup, cloud storage, SaaS, …
  - To protect exchanges : file sharing, email
- *Competencies:*
  - Developing multi-OS products
  - System and network skills to provide transparent encryption to users
- *Interest for the event:*
  - To look for the next wave of cryptographic protocols
  - To prepare our products for them

NOW: THALES UK, RESEARCH &TECHNOLOGY (ADRIAN WALLER) NEXT: SNT, APSIA GROUP, UNIVERSITY OF LUXEMBOURG PETER B. ROENNE

General information

Thales UK, Research and Technology
Adrian Waller
adrian.waller@uk.thalesgroup.com
+44 (0)118 923 8304

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	Y
○ 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	Y*
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	Y
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	Y

Competencies

- *Organisation competencies*
  - **Implementation of cryptographic algorithms and devices (Hardware Security Modules (HSM)s, Key Managers, Network/Link layer Secure Communications,…)**
  - **Application of cryptography in real-world scenarios (practical constraints, system architectures, security management, …)**
- *Organisation experience in the European project*
  - **Extensive across many technology and application areas. In cryptography, current projects include:**
  - **EC H2020 SAFEcrypto (“Quantum Safe” cryptography) – WP Leader, Standards Liaison Manager**
  - **EC H2020 HEAT (Homomorphic Encryption) – WP Leader**
- *The skills you can bring*
  - **Knowledge of implementation techniques, technologies, constraints, assurance, etc.**
  - **Use cases from across the Thales Group (Aerospace, Security, Transport (Road/Rail/Maritime), Space,…)**

not mandatory slide

Project idea

- *Describe your project idea*

- *List of the complementary skills you need for your consortium*

NOW: SNT, APSIA GROUP, UNIVERSITY OF LUXEMBOURG (PETER B. ROENNE) NEXT: UNIVERSITY OF BATH (ALSO OXFORD) (JAMES DAVENPORT)

General information

SnT, APSIA group, University of Luxembourg

Peter B. Roenne

peter.roenne@uni.lu

+352 466644 5079

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	Y
○ 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	Y
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	Y
○ **Quantum key distribution**	**Y**
○ Automated proof techniques for cryptographic protocols	Y

Competencies

- *Broad knowledge and experience in cryptography at expert level*
- *Experience from other European projects*

Project idea

Quantum Key Distribution (QKD)

- *Novel protocols*
  - **Security against stronger adversaries**
  - **Deniability**
  - **Coercion-resistance**
  - **Embedding in standard crypto, e.g. PKI, for enhanced properties**
  - **Authentication protocols, Q-AKEs**
  - **Fairness in Quantum Protocols**

- *List of the complementary skills you need for your consortium*
  - **Partners especially with knowledge on experimentation and validation**

NOW: UNIVERSITY OF BATH (ALSO OXFORD) (JAMES DAVENPORT)

NEXT: CEA LIST (FLORENT KIRCHNER)

HORIZON 2020
LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

Organisation logo

General information

Company name University of Bath (also Oxford)

Contact name James Davenport

Email J.H.Davenport@bath.ac.uk

Telephone number +44-780-872-1953

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	N
○ Authenticated encrypted token research for mobile payment solution	N
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	Y
○ 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

Organisation logo

Competencies

- *Organisation competencies* Mathematics (esp. Number Theory and Algebraic Geometry), Computer Science (Cryptography, Formal Methods)
- *Organisation experience in the European project* 32 years experience of European research funding, dedicated project management and finance teams.

- *The skills you can bring* Davenport has 34 years experience of cryptography and 32 years of European funding. He and colleagues have published on attribute-based authentication/encryption ("I don't care who it is, I need to know that they're authorized"), which is a better fit for many scenarios (Cloud, in particular) than standard identity-based methods.

NOW: CEA LIST (FLORENT KIRCHNER) NEXT: INESC-ID (PAULO MARTINS)

General information

List, a CEA Tech Institute

Florent Kirchner (florent.kirchner@cea.fr) – Software Security

Alexis Olivereau (alexis.olivereau@cea.fr) – Network Security

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	
○ Physical cryptanalysis, including tampering, side channel, faults injection attacks, and security of tools for good software implementation and validation practices	
○ Authenticated encrypted token research for mobile payment solution	
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	Y
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	Y
○ Quantum key distribution	
○ Automated proof techniques for cryptographic protocols	Y

Competencies

- *Organization competencies*
  - **RIA leadership and membership, CSA membership**
  - **active members of ENISA's NIS WG3, PPP Agenda, Allistene, ACN, IETF**
- *10+ years of European project experience:*
  - **OPEN TC (FP6): formal verification of Trusted Computing components**
  - **STANCE (FP7): formal code analysis for cybersecurity**
  - **RISC (H2020): models for the convergence of physical and cybersecurity**
  - **VESSEDIA (H2020): verification engineering for dynamic industrial systems**
  - **CHEKOFV (DARPA): gamifying and crowd-sourcing formal verification**
  - **TWISNet (FP7) , IoT-A (FP7), etc. : Lightweight network security for the IoT**
  - **and also eConfidential, OPEES, MBAT, IngoPCS, Anastasec, Aurochs, …**
- *What we can bring*
  - **Formal verification and validation techniques**
  - **Source and binary code analysis, Runtime monitoring**
  - **Applied to cryptographic primitives and middleware**
  - **As a refinement of higher-level verifications (e.g. Coq, Isabelle, Easycrypt)**
  - **Applied cryptographic primitives (ABE, proxy re-encryption, signcryption…)**
  - **Lightweight crypto-based security protocols (secure delegation, pre-computation…)**
  - **Quantum safe cryptography**
  - **Privacy-preserving approaches (anonymization, pseudonymity…)**

not mandatory slide

Project idea

- *Describe your project idea*
- *List of the complementary skills you need for your consortium*

NOW: INESC-ID (PAULO MARTINS) NEXT: INTELLIGENT VOICE (GÉRARD CHOLLET)

General information

Company name INESC-ID

Web site http://www.inesc-id.pt/

Contact name Paulo Martins (PhD Student) / Leonel Sousa (Senior Researcher)

Email paulo.sergio@netcabo.pt / las@inesc-id.pt

Telephone number +351968548205 / +351969737935

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

Competencies

- *Organisation competencies*
  - *Excellent Research*
  - *Integration with Advanced Education*
  - *Experience in Technology-Transference*
- *Organisation experience in the European project*
  - *Ongoing European Projects:*
    - *Personalised Centralized Authentication System (PCAS)*
    - *Towards the dependable cloud: Building the foundations for tomorrow (DependableCloud)*
    - *Trustful hyper-linked entities in dynamic networks (reThink)*
- *The skills you can bring*
  - *Expertise in Computer Architectures*
  - *Experience in Developing Highly Performant Cryptography*

Project idea

- *Alternative number representations have been used with RSA and ECC*
  - *e.g. Residue Number System*
    - *High-throughput*
    - *Improve resistence against side-channel attacks*
- *Extend these ideas to Post-Quantum Cryptosystems, such as GGH*
- *Exploit emerging High Performance Computing platforms, such as*
  - *GP-GPUs*
  - *FPGAs*

NOW: INTELLIGENT VOICE (GÉRARD CHOLLET) NEXT: NPC SRL (ENRICO CALLEGATI)

HORIZON 2020

LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

General information

Company name : Intelligent Voice®

Contact name : **Gérard CHOLLET**

Email : gerard.chollet@telecom-paristech.fr

Telephone number : +33145817884

Area of interest	**Choose Y or N**
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	Yes
○ Ultra-lightweight cryptology and ultra-high-speed cryptographic algorithms including quantum cryptography	Yes
○ Physical cryptanalysis, including tampering, side channel, faults injection attacks, and security of tools for good software implementation and validation practices	Yes
○ Authenticated encrypted token research for mobile payment solution	Yes
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	Yes
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	Yes
○ Quantum key distribution	No
○ Automated proof techniques for cryptographic protocols	No

Intelligent Voice®

Competencies

- *Automatic Speech Transcription, Indexing, Searching*

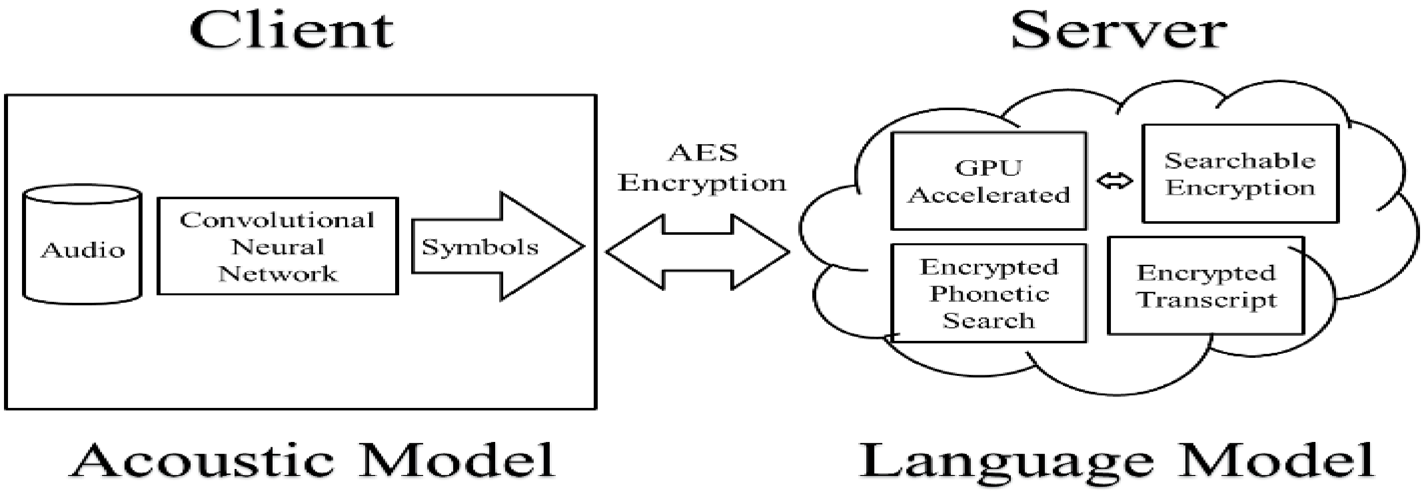
- *Our VP for Research has participated to many European projects since 1983*

- *Automatic speech recognition*
- *Speaker diarisation*
- *GPGPU computing*
- *Symmetric Searchable Encryption*
- *Homomorphic Encryption*

Privacy Preserving Speech Processing

- *The client processes audio to get a lattice of symbols which gets encrypted and sent to the cloud server. He is able to search through encrypted data for strings of symbols.*

- *Looking to crypto specialists*



NOW: NPC SRL
(ENRICO CALLEGATI)
NEXT: E-GROUP ICT SOFTWARE CO.
(MÁRTON CSAPODI)

General information

Company name: NPC Srl

Contact name: Enrico Callegati

Email: callegati.e@crit-research.it

Telephone number +39 059 776865

Area of interest	Choose Y or N
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	N
○ 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	Y
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	Y
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	N
○ Quantum key distribution	Y
○ Automated proof techniques for cryptographic protocols	N

Competencies

- *NPC - SpaceMind Division:*
  - R&D of products dedicated to space sector.
  - Team → Msc Aerospace Engineers with background in space technologies and experience in nanosatellite cubesat class missions
  - The business idea of Spacemind is to become a solution provider for nanosatellite applications. The synergy between the scientific competence of Spacemind and the supply competence of NPC is a key element to offer a complete package of solutions in aerospace applications, permitting to bring a scientific research to a commercial industrialized product and service.
  - Currently Spacemind is developing two important products, besides offering a wide range of services:

    ARTICA: a plug and play deorbiting sail for Cubesat application.

    MORAL: High performances ALT-AZ mount for 1m class telescope and pointing instrument.
- *No direct experience in H2020 but can rely on competent consultant (CRIT Srl)*

not mandatory slide

Qcomm Mission

- *Nanosatellite CubeSat mission for obtaining secure space communication, based on quantum key distribution*
- *Value added:*
  - Improved performance in terms of communication range (no distance limits)
  - Phisically-logistically complicated to interphere with signal
  - Low investment needed – easy to create a sustainable business model (2MLN Eur as turnkey solution once industrialised)
- *Challenges:*
  - Optics & quantum generator miniaturisation for satellite integration
  - Performance assurance
- *Technical partners:*
  - Universtiy of Padua

The idea can be integrated in an existing proposal

NOW: E-GROUP ICT SOFTWARE CO. (MÁRTON CSAPODI) NEXT: BEN GURION UNIV. OF THE NEGEV (YOSSI OREN)

E-GROUP
SOFTWARE & BEYOND

General information

E-Group ICT Software Co. (www.egroup.hu)

Márton CSAPODI	*Áron SZABÓ*
marton.csapodi@egroup.hu	*aron.szabo@egroup.hu*
+36203900857	*+36705054060*

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	N
○ Authenticated encrypted token research for mobile payment solution	Y
○ 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	Y
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	N

Competencies

- *Management owned since 1993, founder & CEO: Antal KUTHY*
- *SW development, security focus, not resellers*
- *Professional team (SW architects, developers, consultants)*
- *Relevant products and competencies: Transacting, eID & PKI*
- *Clients: Financial/Banking/Payment, Government, Energy/Utilities*
- *International sales: SW project experience in 10+ countries*
- *East-West partnerships: www.fisglobal.com, www.unionpay.com*
- *Existing SW stacks: Coriba internet banking, Abaqoos payment, National eID (eIDAS)*
- *In-house technology lab: implementing X.509 certificates for post quantum crypto, Java card blockchain wallet*
- *Innovation labs & partnering with universities, research groups*
- *Several national (HU) and European R+D+I projects*
- *Member in EIT Digital & EIT Health*

Project idea

- *Possible fields of E-Group contribution*

- *Tokenized payment:*
  - **Extend payment (credit card data) tokenization and tokenization service infrastructure to sensitive consumer data at retailers and e-commerce service providers**

- *Quantum safe crypto:*
  - **How to manage change to post-quantum crypto algorithms in the present real life X.509 based technology stacks**
  - **How eIDAS and GDPR regulation and implementation are affected by post-quantum crypto**

NOW: BEN GURION UNIV. OF THE NEGEV (YOSSI OREN)
NEXT: SIMULA@UIB (HÅVARD RADDUM)

Ben-Gurion University of the Negev

General information

Company name: Ben Gurion Univ. of the Negev

Contact name: Dr. Yossi OREN

Email: yos at bgu.ac.il

Telephone number: +972-8-647-9344

Webpage: https://iss.oy.ne.ro

Area of interest	Choose Y or N
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	N
○ **Ultra-lightweight cryptology and ultra-high-speed cryptographic algorithms including quantum cryptography**	Y
○ **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

- ***BGU** is a public research university with over 20,000 students, nationally designated center of excellence in cyber security*
- ***BGU** is a coordinator and partner in over 40 FP funded projects (CIG, ITN, IAPP, IRSES & IF) and MCAs in FP7 and H2020*
- ***My competencies**: Side-channel attacks in unexpected places, constraint solvers for sec., low-power crypto for RFID tags*
- ***Other researchers in BGU**: cryptographic theory (secure distributed computation), IoT sec., malware lab, network sec.*

NOW: SIMULA@UIB (HÅVARD RADDUM) NEXT: NXP SEMICONDUCTORS (FLORIAN BOEHL)

simula@uib

General information

Simula@UiB – Forskningssenteret for Informasjons-og kommunikasjonssikkerhet

Contacts –

- **Håvard Raddum** **haavardr@simula.no**
- **Øyvind Ytrehus** **oyvindy@simula.no**
- **Kjell Jørgen Hole** **hole@simula.no**

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	Y
○ Physical cryptanalysis, including tampering, side channel, faults injection attacks, and security of tools for good software implementation and validation practices	N
○ Authenticated encrypted token research for mobile payment solution	Y
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	Y
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	Y
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	Y

simula@uib

Competencies

- *Organisation competencies/Skills we can bring:*
  - Cryptography and cryptanalysis
  - Information and coding theory
  - Software security

- *Organisation experience in the European project:*
  - As company: Limited (new company, started June 1)
  - Have been partners in NESSIE, ECRYPT, Marie Curie, other projects…

Project idea

- *Functional encryption for cloud databases*
  - Main components: Functional encryption, Efficient implementation, Privacy-preservation , Quantum safe cryptography, Automated proof techniques for FE
  - Simula@UiB, UoB, RU Bochum, U Graz, INRIA
- *List of the complementary skills you need for your consortium*
  - Development to technology readiness level 3-5
  - Stakeholders: regulators, users

Functional Encryption for Cloud Databases

Goal: Implement useful Functional Encryption schemes for cloud computing

Research:

- **Functional Encryption, realisations**
- **Fully Homomorphic Encryption schemes, efficiency and security**
- **Privacy-preserving mechanisms in a cloud computing environment**

Want to be quantum safe

Intend to implement solution(s) using quantum safe crypto:

- **Lattice based and coding based crypto**
- **Encryption schemes based on MQ problem**
- **Ring Learning With Errors**

Consortium

We have:

- **Academic partners with high expertise in cryptography research (TU Graz, RU Bochum, INRIA, UoBergen)**

We need:

- **Partner(s) with expertise in implementing advanced cryptography (industry)**
- **Stakeholder/end-user(s) who would benefit from a functional encryption solution**

NOW: NXP SEMICONDUCTORS (FLORIAN BOEHL) NEXT: NPC SRL (ENRICO CALLEGATI)

General information

❑ NXP Semiconductors

❑ Miroslav Knezevic Florian Boehl Ilya Kizhvatov

❑ miroslav.knezevic@nxp.com florian.boehl@nxp.com ilya.kizhvatov@nxp.com

Area of interest	**Interested**
o Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	*Y*
o Ultra-lightweight cryptology and ultra-high-speed cryptographic algorithms including quantum cryptography	**Y**
o Physical cryptanalysis, including tampering, side channel, faults injection attacks, and security of tools for good software implementation and validation practices	**Y**
o Authenticated encrypted token research for mobile payment solution	*Y*
o Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	**Y**
o New techniques, such as quantum safe cryptography, which are secure from quantum computers	**Y**
o Quantum key distribution	N
o Automated proof techniques for cryptographic protocols	*Y*
Y = definitely interested / *Y* = depends on direction of proposal / N = rather not interested	

Competencies

- NXP’s Innovation Center for Crypto & Security employs > 120 security experts; focus areas include
  - physical security (leakage resilience, fault attacks, tamper resistance),
  - (ultra-)lightweight cryptography (PRINCE cipher),
  - privacy-preserving mechanisms for constrained hardware (VCA) and
  - post-quantum cryptography.
- NXP is currently participating in H2020 projects PQCrypto, HEAT, ECRYPT-NET (2 PhD students)
- Besides strong expertise in the focus areas above NXP can offer
  - insights in current practical constraints for cryptographic solutions on embedded devices and
  - an advanced lab environment with bespoke equipment for fault and side-channel attacks and analysis.

NOW: NPC SRL (ENRICO CALLEGATI) NEXT: INRIA RENNES – BRETAGNE ATLANTIQUE (OLIVIER ZENDRA)

General information

Company name: *NPC Srl*

Contacts:

Enrico Callegati	*Niccolò Bellini*
callegati.e@crit-research.it	*n.bellini@ncpitaly.com*
+39 059 776865	*+39 349 1593659*

Area of interest	**Choose Y or N**
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	N
○ 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	Y
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	Y
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	N
○ Quantum key distribution	Y
○ Automated proof techniques for cryptographic protocols	N

NPC
NEW PRODUCTION CONCEPT

Competencies

SPACE MIND

- *NPC - SpaceMind Division:*
  - **Mission** → R&D of products dedicated to the space sector
  - **Team** → Msc Aerospace Engineers with background in space technologies and experience in nanosatellite cubesat class missions
  - **Vision** → To become a turnkey solutions provider for nanosatellite applications
  - Key **Products**:
    - ARTICA: a plug and play deorbiting sail for Cubesat application.
    - MORAL: High performances ALT-AZ mount for 1m class telescope and pointing instrument.

What is an aerospace company doing in a cryptography brokerage event?

- *No direct experience in H2020 but can rely on **competent engineering partner** (CRIT Srl)*

Project idea

*OBJ→ To develop a technology for the implementation of a **QKD communication protocol between CubeSat & Earth***

- QKD communication via **optic fiber** has now **intrinsic limit** → **range** (100km) due to photon absorption by cable glass
- Satellite usage can **overcome QKD limits**:
  - Improved performance in terms of **communication range** (no distance limits) as photons only cross the atmosphere
  - Phisically-logistically **complicated to interfere**
- Challenges:
  - Optics & quantum generator **miniaturisation for satellite integration**
  - **Performance** assurance (pointer accuracy, link-bdg.)
  - Devices (satellite receiver, telescope) **customisation**
- Exploitation vision (→ 2MLN€ turnkey solution):
  - Secure communication **service to end users** (i.e. banks)
  - Platform industrialisation for **security solution providers**

- High worldwide interest for laser orbit communication (JPN, NASA, China, **ESA → EDRS satellites working @1.8 Gbit/s**)
- High scientific impact on **several domains** (aerospace, physics, ICT)
- Technical partners → *Univ. of Padua (Public. on single photons sat. exchange [2008], quantic sat. communication [2015])*

Avaiable for integration in ongoing proposals

NOW: INRIA RENNES – BRETAGNE ATLANTIQUE (OLIVIER ZENDRA)
NEXT: RO TECHNOLOGY (LUCIANO BOZZI)

HORIZON 2020
LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

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…

NOW: RO TECHNOLOGY (LUCIANO BOZZI) NEXT: TECHSAT GMBH - NEXEYA GROUP (NICOLAS LESELLIER)

General information

- ❑ **Ro Technology** (ITALY)
- ❑ Luciano Bozzi
- ❑ luciano.bozzi@rotechnology.it
- ❑ +39 342 8942896

Area of interest	Choose Y or N
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	N
○ 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	Y
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	Y
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	N
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	Y

Competencies

❑ Organisation competencies

- ❑ Ro Technology designs and develop embedded systems, monitoring systems and applications for ICT, Security, Defense

❑ Relevant European Projects

- ❑ **SafeCOP (ECSEL – Joint Undertaking 2015)**: safety-related cooperating cyber-physical systems, characterised by use of wireless communication and unpredictable operating environments.

❑ Relevant National Projects

- ❑ **Seamless (MoD- PNRM 2015)**: Geo-referenced system for the acquisition of data over a secure, encrypted and energy-efficient WSN .

❑ Specific relevant skills

- Embedded Systems, with particular focus on WSN, IoT and security
- Communication protocols, ICT, SW/FW Design and development
- Monitoring Web applications, OGC services, Requirements engineering, AIV

NOW: TECHSAT GMBH - NEXEYA GROUP (NICOLAS LESELLIER) NEXT: UNIVERSITY OF HAIFA (ORR DUNKELMAN)

techSAT A NEXEYA company NEXEYA

General information

Company name	*TechSAT GmbH (Nexeya group)*
Contact name	*Nicolas Lesellier*
Email	*nicolas.lesellier@techsat.com*
Telephone number	*004917622062291*

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	Y
○ 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	Y
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	Y
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	N
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	Y

Competencies

- *Organisation competencies*
  - **Software (embedded) development**
  - **Embedded Linux development**
  - **Hardware development**
  - **GARDT® technology for secure data loaders validated by Airbus**

- *Organisation experience in the European project*
  - **Sub-partner of CleanSky-2**
  - **Partner of STEVE LuFo (Virtual Hybrid Testing Next Generation)**

- *The skills you can bring*
  - **Architecture of secure systems**
  - **Embedded software/Linux development**

NOW: UNIVERSITY OF HAIFA (ORR DUNKELMAN) NEXT: AIRBUS DS – SECURE LAND COMMUNICATION (CHRISTOPHE CALVEZ)

HORIZON 2020
LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

General information

University of Haifa
Prof. Orr Dunkelman
orrd@cs.haifa.ac.il
+972-4-828-8447

Area of interest	Choose Y or N
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	N
○ Ultra-lightweight cryptology and ultra-high-speed cryptographic algorithms including quantum cryptography	Y
○ 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

- *Design and Cryptanalysis of Symmetric-Key Primitives*
- *Proven track record in the design and analysis of lightweight schemes*
- *Development and Implementation of Real-Life software and hardware designs*

- *Current participation: PQCRYPTO (ICT-645622) and COST action CRYPTACUS (IC 1403)*
  - **Past participation in NESSIE (IST-1999-12324), ECRYPT (IST-2002-507932) , ECRYPT2 (ICT-2007-216676)**

- *Speaking both "Crypto" and "Security"*
- *Understanding "Market Needs" and Engineering aspects, as well as future directions in computing*

- *[Team includes Prof. Shay Gueron (Math dept. + Intel Corp.)]*

NOW: AIRBUS DS –
SECURE LAND COMMUNICATION
(CHRISTOPHE CALVEZ)
NEXT: OPPIDA
(SYLVAIN RUHAULT)

General information

AIRBUS DS SLC (Secure Land Communication)

Christophe CALVEZ

christophe.calvez@airbus.com

+33 1 61 38 78 81

Area of interest	Choose Y or N
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	N
○ Ultra-lightweight cryptology and ultra-high-speed cryptographic algorithms including quantum cryptography	Y
○ Physical cryptanalysis, including tampering, side channel, faults injection attacks, and security of tools for good software implementation and validation practices	N
○ 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	Y
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	Y

Competencies

- *Organisation competencies*
  - Professional Mobile Radio manufacturer for more than 20 years (TETRA/TETRAPOL/P25),
  - Develop network infrastructure and radio terminal products with secured communications needs *(End to End encryption, authentication, HW crypto module …),*
  - Several Public Safety nationwide networks installed all over the world,
  - Competences in security, algorithm/cryptography design and implementation.

- *Organisation experience in the European project*
  - Involved in projects like : SALUS, SOAPS, ISITEP, EPISECC, SECINCORE

- *The skills you can bring*
  - Crypto expertise and implementation
  - Security and cryptography use cases
  - Secured communications solutions and expertise

Project idea

- *Describe your project idea*

⇒ *(can also be a use case attached to another project).*

  - The PMR network are going to migrate from narrowband (TETRA/TETRAPOL) to broadband (LTE/3GPP MCxx) technology (*under standardisation*)
  - New broadband solution and Mission Critical services are based on IBE cryptography mechanisms (*MIKEY-SAKKE*) for key distribution and symmetric algorithm for media encryption,
  - Project / use cases could be to :
    - Analyse and propose security/crypto improvement for the future standardisation releases
    - Analyse, propose and perform feasibility studies for a quantum safe solution

- *List of the complementary skills you need for your consortium*
  - To be discussed
    - HW crypto module provider
    - Academic cryptography experts

NOW: OPPIDA (SYLVAIN RUHAULT) NEXT: LABORATOIRE HUBERT CURIEN (VIKTOR FISCHER)

General information

Company name : Oppida

Contact name : Sylvain Ruhault

Contact details : sylvain.ruhault@oppida.fr / 0628566638

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	Y
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	Y
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	N
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	Y

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Competencies

- *Organisation competencies*

  Security testing of IT systems and products
  - **Common Criteria (ISO 15408) evaluations (100 evaluations performed)**
  - **CSPN evaluations (> 50 evaluations performed)**
  - **Cryptographic assessments ((> 50 assessments performed)**

  Licensed by

  arJeL
  Autorité de régulation
  des jeux en ligne

  PCI Security Standards Council
  QUALIFIED SECURITY
  ASSESSOR

- *Research projects*
  - **Industrial systems security (SCADA)**
  - **Attack detection (IDS)**
  - **Cryptography (PRNG analysis)**

- *The skills you can bring*
  - **Common Criteria / code source analysis / reverse / pen tests**

Organisation logo

not mandatory slide

Project idea

- *Describe your project idea*
- *List of the complementary skills you need for your consortium*

NOW: LABORATOIRE HUBERT CURIEN (VIKTOR FISCHER)
NEXT: BARCO SILEX (THIERRY WATTEYNE)

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

H2020 – 5 Septembre 2016

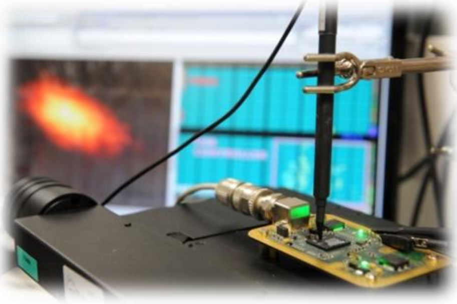
Equipe Systèmes Embarqués Sécurisés et Architectures Matérielles (SESAM)

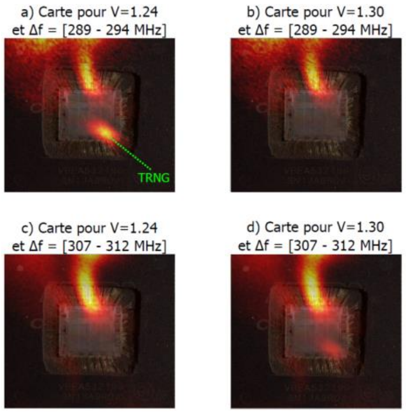
Viktor Fischer, Lilian Bossuet

Objectifs scientifiques

Conception de générateurs d'aléa (TRNG) et de fonctions physiques non clonables (PUF) pour la cryptographie

- Etude des sources d'aléa dans les circuits logiques (technologie CMOS)
- Méthodes, outils et modèles mathématiques utilisés pour caractériser l'aléa et son extraction
- Proposition de test embarqués permettant de tester les générateurs d'aléa en ligne
- Evaluation de la sécurité des générateurs d'aléa (attaques par injection de fautes et/ou analyse des canaux cachés)
- Application à la lutte contre la contrefaçon et le vol de circuits intégrés et d'IP





a) Carte pour V=1.24 et Δf = [289 - 294 MHz]

b) Carte pour V=1.30 et Δf = [289 - 294 MHz]

c) Carte pour V=1.24 et Δf = [307 - 312 MHz]

d) Carte pour V=1.30 et Δf = [307 - 312 MHz]

Architecture matérielles résistantes aux attaques cryptographiques passives et actives

- Architectures de crypto-processeurs incluant la gestion sécurisée des clés
- Architectures de systèmes cryptographiques post-quantiques résistantes aux attaques par analyse de canaux cachés

Equipe & collaborations européenes

Effectifs

- 2 Professeurs des Universités, 4 Maîtres de Conférences
- 1 Ingénieur de recherche du CNRS
- 6 Doctorants et 2 Post-doctorants

Projets collaboratifs européens

- EIT IAMIT - Identity and Access Management for the Internet of Things
  - SICS, UJM, TU Berlin, Ericsson, Deutsche Telekom

eit Knowledge & Innovation Community
EIT ICT Labs

- H2020 HECTOR - Hardware Enable CrypTO and Randomness
  - KU Leuven, UJM, TU Graz, STMicroelectronics, Thales C & S, Brigtshight, Micronic, Technikon

HORIZON 2020
LE PORTAIL FRANÇAIS DU PROGRAMME EUROPÉEN POUR LA RECHERCHE ET L'INNOVATION

- COST ACTION TRUDEVICE – Trustworthy Manufacturing and Utilization of Secure Devices

cost
EUROPEAN COOPERATION IN SCIENCE AND TECHNOLOGY

NOW: BARCO SILEX (THIERRY WATTEYNE) NEXT: UNIVERSITY OF CAMBRIDGE, CENTRE FOR PHOTONIC SYSTEMS (ADRIAN WONFOR)

HORIZON 2020
LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

BarcoSilex

General information

Barco Silex *Thierry Watteyne*

Thierry.Watteyne@barco.com

+ 32 475721546

HW accelerated embedded security

Barco Silex is a Belgian company specialized in the development of embedded electronics based upon FPGA and SoC technologies, with a strong expertise in cryptography and data security , as well as on video encoding and image processing

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	Y
○ 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	Y
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	N

BarcoSilex

Competencies

Proposed expertise or activities to offer:

- Hardware acceleration cryptography for data security in embedded systems (Root-of-trust, TEE, TLS/SSL/VPN offloading, disk encryption…)
- Comprehensive embedded security platforms (HW&SW) for integrated systems (SoC)
- SoC development skills
    - Chip design
    - SoC FPGA design

Areas:

Implementation of novel cryptographic architectures

Integration in embedded security subsystems for:

- IoT, Wearables
- Connected vehicles, V2V, V2X
- HSMs for various applications (Government e-security, e-payments, ….)
- High throughput TLS/SSL connections
- High bandwidth networking(IPsec)
- Industrial networking
- Defense
- Data Centers

NOW: UNIVERSITY OF CAMBRIDGE, CENTRE FOR PHOTONIC SYSTEMS (ADRIAN WONFOR)
NEXT: KU LEUVEN - IMINDS - COSIC (DAVE SINGELÉE)

General information

University of Cambridge, Centre for Photonic Systems

Adrian Wonfor, Richard Penty

aw300@cam.ac.uk , rvp11@cam.ac.uk

+44 1223 748355, +44 1223 748358

Area of interest	Choose Y or N
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	N
○ 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	N
○ 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	Y
○ Quantum key distribution	Y
○ Automated proof techniques for cryptographic protocols	N

UNIVERSITY OF CAMBRIDGE

Competencies

- *Extensive expertise in telecommunications and datacommunications*
- *Photonic Integration for optical sources and switches etc.*
- *Partner UK Quantum Communications Hub*

- *Many EU projects for photonic integration, communications (PONs Long Haul telecoms etc.) Energy efficient communications*

- *Test-beds and demonstrators for combination of QKD with encrypted conventional traffic*
- *Cambridge Quantum Network demonstrator (QKD and high data-rate (Multiple 100Gb/s) telecoms flexible topology network within Cambridge).*
- *Partner in UK national dark fibre network NDFIS (QKD compatible)*
- *Dedicated QKD enabled link to BT labs Adastral Park*

Site for QKD test-beds

- *Large QKD compatible test-beds.*
- *Within Cambridge (30km), to BT (150km), UK Dark Fibre Network (500km)*

- *Experimental group with extensive communications experience, with 100Gb/s transmission systems and QKD equipment from major vendors (ID Quantique and Toshiba)*

NOW: KU LEUVEN - IMINDS - COSIC (DAVE SINGELÉE) NEXT: MIRACL (MICHAEL SCOTT)

General information

KU Leuven - iMinds - COSIC
Dave Singelée (research manager)
Dave.Singelee@esat.kuleuven.be
www.esat.kuleuven.be/cosic

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	Y
○ 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	Y
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	Y
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	Y
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	N

Competencies

- *Electrical Engineering department @ KU Leuven*
- *5 professors, +/- 70 researchers*
- *Head of the group: prof. Bart Preneel*

- *Participation in over 45 European research projects (9 as coordinator)*
- *Currently 7 ongoing H2020 projects*

- *Strong expertise in*
  - **Cryptography**
  - **Privacy-enabling technologies**
  - **Embedded Security**
- *Research Interests*
  - **Lightweight cryptography, post-quantum crypto, authenticated encryption, PETs, Secure Multi-Party Computation, side-channel and fault injection attacks, HW roots of trust, etc.**

NOW: MIRACL
(MICHAEL SCOTT)

HORIZON 2020
LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

General information

MIRACL.com

Mike Scott

Mike.scott@miracl.com

+353 86 3888746

Area of interest	Choose Y or N
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	N
○ Ultra-lightweight cryptology and ultra-high-speed cryptographic algorithms including quantum cryptography	Y
○ 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	Y
○ 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	Y
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	N

Competencies

- *Pairing based Crypto and Authentication*
- *Previous involvement in EU projects and proposals*
- *Elliptic Curve/Pairing-Based Crypto skills, efficient implementations*