
https://cybersecurity.ulb.be

# Master Theses Proposals

## — Network Security—

## 2022-2023

# Physical-layer security — IoT device authentication and ciphering using physical unclonable functions

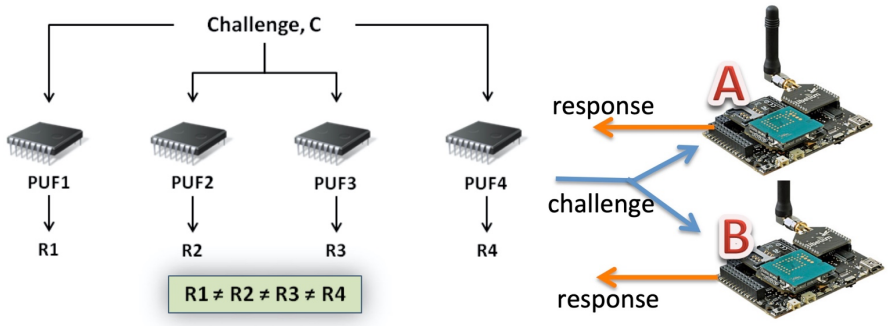
Information: Jean-Michel Dricot, Dragomir Milojevic, Olivier Markowitch

## MOTIVATION

There are approximately 50 billion of IoT devices in the world today and their number grows aggressively over the years. With their large level of deployment comes the need of protecting these devices from malicious since IoT (in)security is a major problem and a rising threat (see for instance the Mirai botnet attack). In practice, there is a strong need to implement lightweight authentication and ciphering of the communication beyond classical crypto protocols, such as Diffie-Hellman key exchange or TLS that are out of the reach of embedded electronics.

A physical unclonable function (PUF) is a device that exploits inherent randomness introduced during CMOS manufacturing to give a physical entity a unique fingerprint of the device (similar to human biometrics). PUFs are most often based on unique physical variations which occur naturally during semiconductor manufacturing but can also be embodied in side electronics designed for that purpose. Examples include clock drifts, SRAM memory states, logical gates response, etc.

From a security perspective, any challenge presented to a device will lead to a different response, based on the unique characteristics of the electronics (see fig. below) and can be exploited to perform identification, signing, and key derivation.




*Device fingerprinting at physical layer*

## OBJECTIVES

- Understand the core concepts of physical unclonable function and its application in the context of Internet of Things.
- Demonstrate using a FPGA-based implementation and analyse its sensitivity to the environment (e.g. power-up cycles, temperature) .
- Identify your device with its unique fingerprint and the corresponding fuzzer (a “correction” function to stabilize the input and output)

## CONTACT

Jean-Michel Dricot (jean-michel.dricot@ulb.be), D. Milojevic dmilojev@ulb.ac.be

# Physical-layer security — Physical unclonable functions from and for commodity hardware

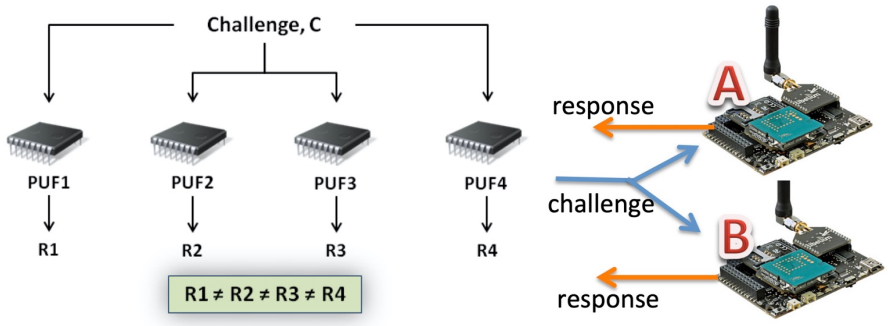
Information: Jean-Michel Dricot, Dragomir Milojevic
Type: Theoretical and/or experimental

## MOTIVATION

There are approximately 50 billion of IoT devices in the world today and their number grows aggressively over the years. With their large level of deployment comes the need of protecting these devices from malicious since IoT (in)security is a major problem and a rising threat (see for instance the Mirai botnet attack). In practice, there is a strong need to implement lightweight authentication and ciphering of the communication beyond classical crypto protocols, such as Diffie-Hellman key exchange or TLS that are out of the reach of embedded electronics.

A physical unclonable function (PUF) is a device that exploits inherent randomness introduced during CMOS manufacturing to give a physical entity a unique fingerprint of the device (similar to human biometrics). PUFs are most often based on unique physical variations which occur naturally during semiconductor manufacturing but can also be embodied in side electronics designed for that purpose. Examples include clock drifts, SRAM memory states, logical gates response, etc.

From a security perspective, any challenge presented to a device will lead to a different response, based on the unique characteristics of the electronics (see fig. below) and can be exploited to perform identification, signing, and key derivation.




*Device fingerprinting at physical layer*

## OBJECTIVES

- Understand the core concepts of physical unclonable function and its application in the context of Internet of Things.
- Investigate how commodity hardware can be exploited / extended in order to embed PUF.
- Deliver an implementation (e.g. SRAM-based PUF key derivation and authentication architecture) on a RaspberryPi box.

## CONTACT

Jean-Michel Dricot (jean-michel.dricot@ulb.be) and Dragomir Milojevic dmilojev@ulb.ac.be

# Physical-layer security — WiFi channel authentication

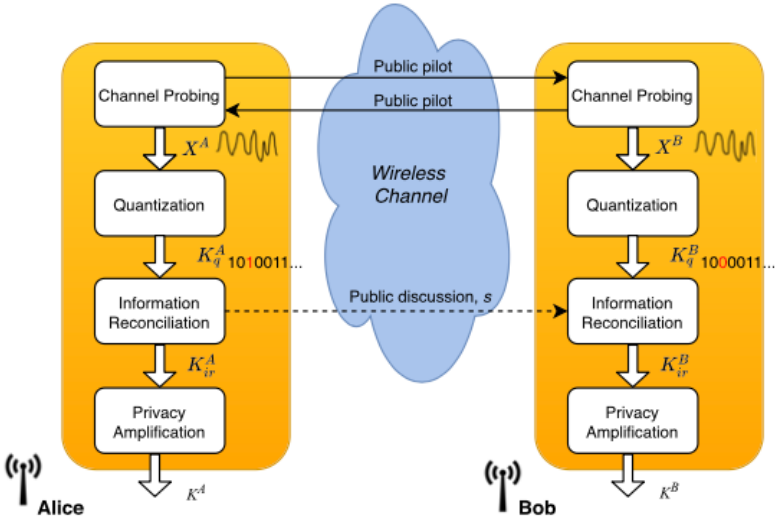
Information: Jean-Michel Dricot
Type: Theoretical and/or experimental

## MOTIVATION

In 2017 was discovered a weakness in WPA2, the protocol that secures all modern protected Wi-Fi networks. An attacker within the vicinity of a victim could intercept the key exchange phase and force a key re-installation, hence leading to insecure communication (possibly zeroing the key).

This attack makes use of a channel-based MitM attack, where the rogue access point is cloned on a different channel with the same MAC address as the targeted access point. A practical counter-measure to this is channel authentication, i.e., use the physical properties of the wireless channel (i.e., reciprocity) to determine if a relaying antenna has been inserted or not between the terminals.

A previous and successful master thesis conducted in our lab showed that a shared secret key can be silently computed by Alice and Bob (without any exchange of information). Then, this key can be used to authenticate the communication channel and/or bootstrap a key scheduling for crypto.




*Wireless channel fingerprinting and key derivation*

## OBJECTIVES

- Understand the core properties of wireless physical transmission and its application to security
- Implement a permanent proof-of-concept for WiFi systems with a channel signature scheme or channel authentication scheme
- Demonstrate by implementing a CRACK-resistant variant of WPA2 protocol based on channel authentication

## CONTACT

Jean-Michel Dricot (jean-michel.dricot@ulb.be)

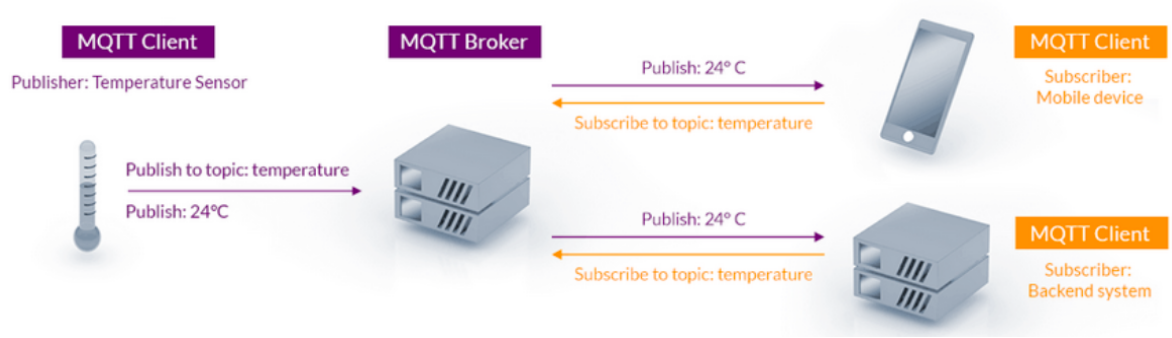
# Privacy-aware data collection for the Internet of Things

Information: Jean-Michel Dricot
Type: Theoretical and/or experimental

## MOTIVATION

The growing expectations for ubiquitous sensing have led to the integration of countess embedded sensors, actuators, and RFIDs in our surroundings. Combined with rapid developments in high-speed wireless networks, these resource-constrained devices are paving the road for the Internet-of-things paradigm, a computing model aiming to bring together millions of heterogeneous and pervasive elements. However, it is commonly accepted that the Privacy consideration remains one of its main challenges, a notion that does not only encompasses malicious individuals but can also be extended to honest-but-curious 3rd parties.

This master thesis' goal is hence to study and apply various Privacy-enhancing Technologies (PET) to MQTT, a highly popular lightweight publish/subscribe communication protocol. The student will proposes a secure communication protocol which ensures that no valuable information can be extracted from the messages flowing through the broker. In addition, it also prevents partners re-identification.




*MQTT data broker (honest but curious) in the Internet of Things*

## OBJECTIVES

- Understand the core requirements of privacy-aware tracking and the use of physical unclonable function in key schedule.
- Design a reliable, privacy preserving tracking protocol that inherently avoids de-anonymization while allowing to verify medical accuracy of the information.
- Implement in the form of an app in a smartphone.

## CONTACT

Jean-Michel Dricot (jean-michel.dricot@ulb.be)

# Offline key agreement for autonomous Smart Grids

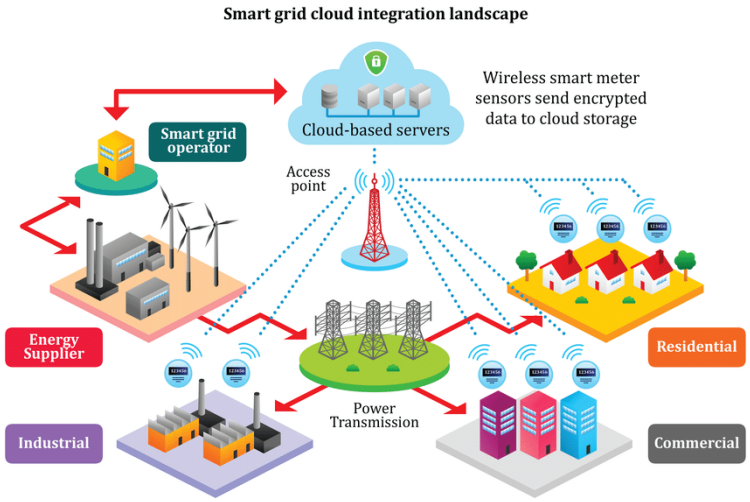
Information: Jean-Michel Dricot
Type: Theoretical and/or experimental

## MOTIVATION

The Internet of Things (IoT) comprises more than 50 billion connected devices and are used everywhere, from smart home devices to building automation, in healthcare, in the industry 4.0. Due to this exponential growth of IoT, there are serious questions about these devices' security and privacy. Key-management hence becomes of utmost importance to allow various devices to pair with one another without revealing any security-sensitive data to the environment.

When pairing IoT devices, one often relies on the implicit assumption that all the IoT devices are online during the pairing process and can authenticate to each other. However, it very likely in some scenarios that the device are not online for a long period of time (e.g. during a cyber attack) or mostly disconnected from a master device (autonomous IoT). Some scenarios in the domain of Smart Grids consider disconnecting "islands" of the energy grids to increase the resilience to attacks.

The objective is to design an authentication and key derivation architecture that allows to securely bootstrap and pair devices that cannot interactively communicate during the initialization of the network.




*Smar grids as connected and autonomous islands*

## OBJECTIVES

- Study the underlying network architectures and cryptography to solve the disconnection problem (e.g. offlkine key derivation functions -KDF- and Ratchet algorithms).
- Design a reliable key derivation protocol for smart grids.
- The student can also try to guarantee additional security goals such as perfect forward secrecy, forward anonymity, or backward secrecy.

## CONTACT

Jean-Michel Dricot (jean-michel.dricot@ulb.be)

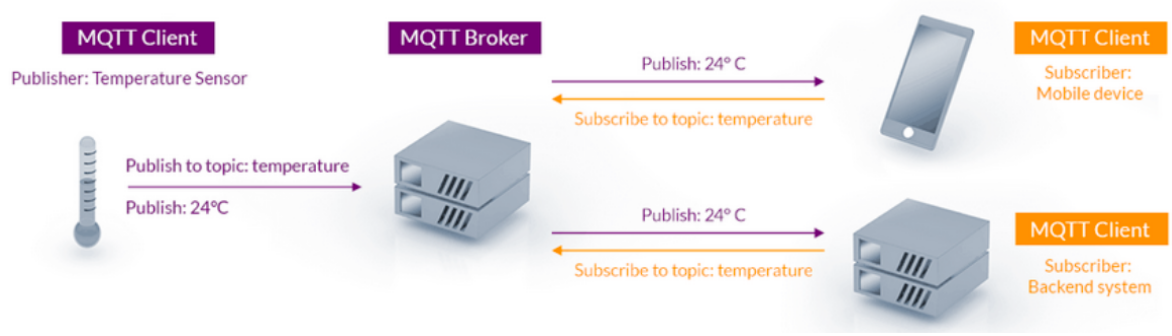
# Privacy-aware data collection for the Internet of Things

Information: Jean-Michel Dricot
Type: Theoretical and/or experimental

## MOTIVATION

The growing expectations for ubiquitous sensing have led to the integration of countess embedded sensors, actuators, and RFIDs in our surroundings. Combined with rapid developments in high-speed wireless networks, these resource-constrained devices are paving the road for the Internet-of-things paradigm, a computing model aiming to bring together millions of heterogeneous and pervasive elements. However, it is commonly accepted that the Privacy consideration remains one of its main challenges, a notion that does not only encompasses malicious individuals but can also be extended to honest-but-curious 3rd parties.

This master thesis' goal is hence to study and apply various Privacy-enhancing Technologies (PET) to MQTT, a highly popular lightweight publish/subscribe communication protocol. The student will proposes a secure communication protocol which ensures that no valuable information can be extracted from the messages flowing through the broker. In addition, it also prevents partners re-identification.




*MQTT data broker (honest but curious) in the Internet of Things*

## OBJECTIVES

- Understand the core requirements of privacy-aware tracking and the use of physical unclonable function in key schedule.
- Design a reliable, privacy preserving tracking protocol that inherently avoids de-anonymization while allowing to verify medical accuracy of the information.
- Implement in the form of an app in a smartphone.

## CONTACT

Jean-Michel Dricot (jean-michel.dricot@ulb.be)

# Fast symmetric cryptography using ARM specialized instructions

Information: Gilles Van Assche, Jean-Michel Dricot, Olivier Markowitch
Type: Theoretical and/or experimental

## MOTIVATION

Recently, ARM™ added special instructions to their ARMv8-A instruction set that aim at accelerating standard cryptographic algorithms. Among these, a small set of instructions targets the acceleration of the Keccak-f permutation inside SHA-3, and it turns out that these instructions are actually fairly general and offer potential use beyond Keccak/SHA-3.

In particular, we believe that these instructions could also accelerate authenticated encryption schemes like Xoofff, although using a non-trivial representation.

## OBJECTIVES

The goal of this master's thesis would be first to evaluate the suitability of the these instruction for Xoofff, for other Farfalle-based schemes and for any other state-of-the-art scheme. Then, the student would implement and benchmark selected schemes on an ARMv8-A platform. Finally, the student would be analyze how to take best advantage of these instructions in the design of new primitives and in particular of new Farfalle-based schemes.

## CONTACT

Gilles Van Assche (gilles.van.assche@ulb.be), Jean-Michel Dricot, and Olivier Markowitch

# High-performance blockchain signatures for e-payment

Information: Jean-Michel Dricot, Gaurav Sharma
Type: Theoretical and/or experimental

## MOTIVATION

ULB and Worldline collaborate to build an innovative blockchain platform which can enhance the performance of blockchain systems comparable to centralized systems. The Worldline's smart payment engine (SPE) facilitating the payments between consumer and merchant banks, is planned to employ blockchain technology to its core architecture and hence decentralize the trust. One of the major challenges is to achieve the desired transaction throughput satisfying the merchants and banks privacy requirements.

The project is about the development of a high-performance permissioned blockchain architecture focusing on three types of transactions. A normal transaction is a public transaction without any privacy focus while private transactions conceal the participant parties as well as the transaction amount. Currently, some existing blockchain platforms facilitate these two types of transactions. However, our objective is to add a new type of transaction which is an outcome of a bidding process, keeping the privacy as the highest priority. The major challenge here is to choose the bidding winner in an extremely efficient way.

## OBJECTIVES

- Produce a proof of concept for an auction/bidding system in a permissioned blockchain environment (Ethereum with Solidity language).
- Implement a protocol with the following properties:
    - Bid privacy. All bidders cannot know the bids submitted by the others before committing to their own
    - Posterior privacy. All committed bids are maintained private from the bidders and public bidders.
- The scientific contribution targeted for this internship is to achieve bidder's privacy but the *highest bidder (winner) is traceable*.

## REFERENCES

[1].Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)* (pp. 839-858). IEEE.

[2]. Galal, H. S., & Youssef, A. M. (2018, February). Verifiable sealed-bid auction on the ethereum blockchain. In *International Conference on Financial Cryptography and Data Security* (pp. 265-278). Springer, Berlin, Heidelberg.

## CONTACT

Denis Verstraeten (Denis.Verstraeten@ulb.be) and Jean-Michel Dricot (jean-michel.dricot@ulb.be)

# Design of a secure vault for the storage of crypto keys at ULB

Information: Jean-Michel Dricot
Type: Analysis and implementation

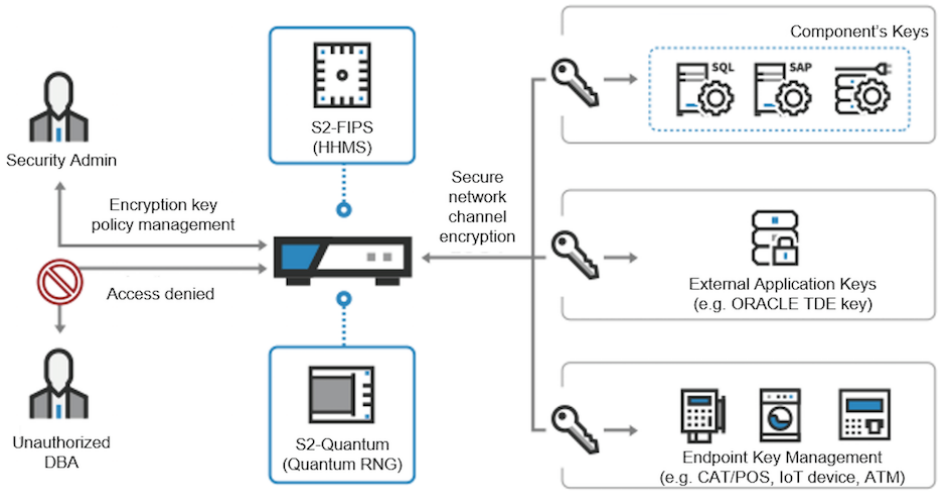
## MOTIVATION

Cryptographic keys are needed in any modern secure implementation. For instance, GDPR compliance requires to provide pseudonymization or anonymization on the manipulated data. To meet that goal, keyed hash technique is used, which implies to instantiate, store, and destroy a key for each person requesting a data extraction. More generally speaking, crypto keys are also used for authentication, encryption, signing, etc.

Secure manipulation is often overlooked by the users. These keys need to be created securely, delivered to the right person (access management), destroyed after a determined period of time. These operations must be properly logged and audited.

## OBJECTIVES

The objective of this thesis is to analyse and implement a secure vault of keys that will be used to pseudonymize some data provided to the researchers by the university. The notarization of these keys will be based on the Vault technology (by HashiCorp).




This work is highly multidisciplinary : business requirement analysis (IT and teaching departments of the ULB), security design (communications, deployment of the Vault, persons of trust to operate and activate the vault), cryptography (key qualities for the defined applications), network (secure architecture as a whole) etc.

## CONTACT

Jean-Michel Dricot (jean-michel.dricot@ulb.be)

# The ULB HOME project — Privacy-preserving location tracking and sharing

Information: Jean-Michel Dricot
Type: Architecture analysis and implementation

## Motivation

Le projet HOME a pour objectif de rendre le milieu festif et la vie nocturne de la communauté étudiante plus sûrs. Il a commencé il y a presque deux ans, et est suivi et soutenu par plusieurs organes de l'ULB, en plus d'ˆêtre unanimement défendu par tous les cercles de l'ULB. Plus précisément, le projet se concentre sur la sécurité lors des retours de sorties ayant lieux sur les sites de l'université et également les endroits à haute fréquentation étudiante. En effet, le sondage que nous avons réalisé à ce sujet a permis de mettre en évidence - grâce à plus de 500 réponses obtenues - la nécessité accrue d'un moyen pour rentrer chez soi en sécurité, et ce sans recourir `a des services payants ou parfois même peu fiables.

## Objectifs

Un groupe d'étudiant.e.s a opté pour le dévleoppement une application mobile, dont le concept principal est le co-piétonage. En formant des groupes d'étudiant.e.s ayant des trajets identiques ou semblables, nous espérons diminuer les risques liés aux trajets de nuit. Une fonctionnalité importante est la communication en temps réel avec ses proches via une *friendlist*. Les personnes ayant été ajoutées comme ami.e ont accès en direct aux informations liées au déroulement du trajet. De plus, le statut *close friend permet* de partager sa localisation en temps réel avec une liste d'ami.e.s proches.

Le but de ce mémoire est (1) de proposer une architecture sécurisée permettant le partage en temps réel de données personnelles (position, messages, etc) sur un mode P2P (semblable à Signal) ; (2) de développer une app iOS/Android qui sera utilisée par les étudiant.e.s pour sécuriser les sorties de soirées.

De bonnes connaissances en cybersécurité sont requises. Une expérience en développement d'app (framework iOS/Android, lifecycle devel-déploy sur les stores) est souhaitée.

Contact étudiant : Grégroy Coolen

Contact Académique : Jean-Michel Dricot

## Some subjects from the previous years….

- Detecting compromised switches in Software Defined Networks
- Cyber range for education and training – collaboration with the Royal Military Academy
- Botnet detection in encrypted traffic – **Award from the Belgian ISP association**
- Implementation of AES in a custom-developed FPGA system (side-channel attacks analysis) – In collaboration with THALES
- Key recovery with SPECTRE and MELTDOWN attacks – In collaboration with the Université de Bretagne Sud (UBS)
- Applying machine learning to detect zero-day attacks
- Integrating Cyber-Attack Defense Techniques into Real-Time Cyber-Physical Systems
- Security analysis of automotive communications
- Security protocols for the Cloud-of-Chips architecture: an ID-based cryptography approach
- Security protocols for the Cloud-of-Chips architecture: a group-based cryptography approach
- Preventing man-in-the-middle attacks in protected Wi-Fi networks (KRACK attack)
- High-performance blockchain signatures for e-payment
- Simulation of smart grids environments….