UMR IRISA

Activity Report 2019

Team EMSEC

Embedded Security & Cryptography

D1 – Large Scale Systems

CentraleSupélec · cnrs · ens rennes · IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom · Inria · INSA Rennes · Université Bretagne Sud ubs · Université de Rennes 1

Contents

1 Team composition

Researchers and Faculty Members

Gildas Avoine (*)	Professor	INSA Rennes
Stéphanie Delaune	Senior Researcher	CNRS
Patrick Derbez	Assistant Professor	Univ. Rennes 1
Barbara Fila	Assistant Professor	INSA Rennes
Pierre-Alain Fouque (*)	Professor	Univ. Rennes 1
Clémentine Maurice	Junior Researcher	CNRS
Adeline Roux-Langlois	Junior Researcher	CNRS
Mohamed Sabt	Assistant Professor	Univ. Rennes 1

(*) Co-leaders

PhD students

Olivier Bernard	Feb 2019 to Jan 2022	H2020 Prometheus
Pauline Bert	Sep 2016 to Sep 2019	Bourse DGA
Angèle Bossuat	Sep 2017 to Sep 2020	Bourse DGA
Katharina Boudgoust	Sep 2018 to Aug 2021	Bourse DGA
Daniel Braga de Almeida	Sep 2019 to Sep 2022	Bourse DGA
Qian Chen	Sep 2016 to Sep 2019	Bourse ENS
Alexandre Debant	Oct 2017 to Sep 2020	ERC POPSTAR
Guillaume Didier	Sep 2019 to Aug 2022	IA DGA
Céline Duguey	Feb 2018 to Jan 2021	DGA Engineer
Gautier Eberhart	Oct 2018 to Sep 2021	H2020 Prometheus
Loïc Ferreira	Oct 2016 to Sep 2019	Orange Labs
Guillaume Kaim	Oct 2017 to Sep 2020	Orange Labs
Paul Kirchner	Mar 2018 to Mar 2021	BPI RISQ + DGA
Baptiste Lambin	Sep 2016 to Sep 2019	Bourse DGA
Solène Moreau	Sep 2018 to Aug 2021	ERC POPSTAR
Victor Mollimard	Sep 2018 to Sep 2021	Bourse ENS
Adina Nedelcu	Mar 2018 to Mar 2021	Orange Labs
Joshua Peignier	Sep 2019 to Aug 2022	ERC POPSTAR
Thomas Rokicki	Oct 2019 to Sep 2022	ANR MIAOUS
Alban Siffer	Sep 2016 to Dec 2019	Amossys
Florent Tardif	Jan 2016 to Jun 2019	Bourse MENRT
Wojciech Wideł	Nov 2016 to Sep 2019	Bourse MENRT

Postdocs

Xavier Bultel	Jul 2018 to Aug 2019	ANR SafeTLS
Adela Georgescu	Jan 2019 to Oct 2020	BPI RISQ
Sam Thomas	Jul 2018 to Jun 2019	Bourse DGA
Tian Tian	Apr 2018 to Sep 2019	Own grant
Vaishnavi Sundararajan	Nov 2018 to Oct 2019	ERC POPSTAR
Weiqiang Wen	Sep 2018 to Aug 2020	H2020 Prometheus
Yang Yu	Apr 2018 to Sep 2019	BPI RISQ + Labex TYREX + Prometheus

Associate members

Benoît Gérard	Sep 2013 to Oct 2022	DGA-MI
Cyrille Wiedling	Sep 2019 to Aug 2022	DGA-MI
Antoine Dallon	Sep 2019 to Aug 2022	DGA-MI

Administrative assistant

Aurélie Patier

2 Overall objectives

2.1 Overview

News reflect the growing importance of cybersecurity, especially cyberattacks. This is unfortunately not a journalistic bias, but a reality that results in an increase in the number of attacks and their impact. If security has grown so much, especially in the last 15 years, this is because IT has become ubiquitous. It is difficult today to have activities that do not rely on computing systems. The Achilles heel is that there is usually no procedure to continue an activity in case of major failure: an airport, for example, can stay stuck when an attack is ongoing.

Members of EMSEC work on different aspects of cryptology, in particular on lattice-based cryptography, symmetric cryptanalysis, and security of protocols. EMSEC is also strongly involved in two important NIST competitions about the security of post-quantum schemes and lightweight ciphers. Formal methods is a complementary approach to verify the security of a protocol or a system. Many examples illustrate that building blocks proven in a computational model can still suffer from weaknesses that are discovered using a symbolic approach. EMSEC consequently considers formal methods for the verification of cryptographic protocols, and development of techniques and tools, relying on attack trees, for quantitative analysis of security and risk assessments of real-life systems. EMSEC also works on the security of hardware and software systems, analyzing the security of cryptographic implementations, especially from a side-channel perspective, and designing and improving attacks, mostly attacks based on microarchitectural covert and side channels, and attacks based on cryptanalytic time-memory trade-offs. Finally, EMSEC considers various topics related to data security and machine learning, new statistical tools to detect shift in a timing series or anomaly, data desanonymization, and forensics applied to smartcards.

2.2 Scientific foundations

EMSEC's research activities are organized along three axes, namely cryptography, formal methods for security, and security of hardware and software systems. These axes are illustrated below with the major topics EMSEC deals, which are described in depth from Section 2.2.1 to Section 2.2.3.

Cryptography: EMSEC addresses the design of secure building blocks based on security proofs and cryptanalysis of such blocks.

- Design of ciphers: lightweight block ciphers, authenticated encryption schemes, etc.
- Lattice-based cryptography, security proofs and advanced constructions
- Cryptanalysis of symmetric and asymmetric constructions, cryptanalytic time-memory trade-off
- Security of cryptographic implementations: side-channel attacks and countermeasures
- Design and cryptanalysis of protocols: distance bounding, SSL/TLS, multi-party contract signing protocols, and protocols for low cost devices (RFID, smartcard, etc.)
- Fully homomorphic encryption, symmetric searchable encryption

Formal Methods for Security: one of the major concerns of information security is to establish security proofs. EMSEC investigates the usage of formal methods as well as the development of novel techniques for reasoning about security.

- Formal proofs for cryptographic protocols: key establishment, distance bounding
- Models for quantitative analysis of security
- Risk analysis based on attack trees
- Cryptanalysis of block ciphers using solvers (CP, SAT, MILP)

Security of Hardware and Software Systems: EMSEC works on finding vulnerabilities in real-world systems, with the aim to provide the security community with valuable feedback and lead to more secure designs.

- Micro-architectural attacks, including side-channel attacks and software-based fault attacks
- Data security & machine learning, including data desanonymisation and forensics in embedded systems
- Smartphone security

2.2.1 Cryptography

Asymmetric primitives. EMSEC is strongly involved in the NIST competition on the security of post-quantum schemes. In particular, we design new signature and ring-signature schemes based on structured and module lattices. Ring-signature is a specific scheme that allows to add anonymity properties since we do not know who signs within a group of users. We also work on the security of cryptographic implementations of lattice schemes. We study the core component of efficient lattice schemes such as Gaussian sampling against timing attack. EMSEC addresses the security of the BLISS signature schemes against various side-channel attack. Since the side-channel information is very low, we need to use statistical tools to amplify the signal. It is very interesting to use machine learning techniques to improve side-channel attacks. We also work on efficient implementations for core operations of Lattice-based constructions, including polynomial multiplication and Gaussian sampling over integers.

Symmetric primitives. EMSEC is also involved in the NIST competition on lightweight ciphers. In particular, EMSEC works on the key schedule of the AES block cipher to introduce more efficient constructions against classical attacks. EMSEC also considers the more powerful white-box model and suggests attacks on proposals as well as generic attacks. Note that EMSEC also considers and refines division property-based attacks on block ciphers such as SKINNY, RECTANGLE and Midori. EMSEC finally studies the resistance of lightweight symmetric ciphers using automatic tools, including MILP or CSP solvers.

To perform attacks, EMSEC also considers cryptanalytic time-memory trade-off (TMTO) techniques. TMTOs were introduced by Martin Hellman in 1980 to reduce the time needed to perform an exhaustive search. The key-point of the technique resides in the precomputation of tables that are then used to speed up the attack itself. Given that the precomputation phase is much more expensive than an exhaustive search, a TMTO makes sense in a few scenarios, e.g., when the adversary has plenty of time for preparing the attack while she has a very little time to perform it, the adversary must repeat the attack many times, or the adversary is not powerful enough to carry out an exhaustive search but she can download precomputed tables. Problems targeted by TMTOs mostly consist in retrieving the preimage of a hashed value or, similarly, recovering a cryptographic key through a chosen plaintext attack.

Design and cryptanalysis of protocols. EMSEC works on various topics related to cryptographic protocols. It so considers attacks and proofs on everyday-life protocols, e.g., TLS 1.3 (especially with respect to middleboxes), LoRaWAN 1.0, SCP02, SCP10, 5G, WPA3 Dragonfly, FIDO U2F, and WhatsApp; and designs of new protocols, e.g., instant messaging protocols, distance-bounding protocols, and secure-routing protocols.

2.2.2 Formal Methods for Security

We strongly believe formal methods is a complementary approach to verify the security of a protocol or a system. Many examples illustrate that building blocks proven in a computational model can still suffer from weaknesses that are discovered using a symbolic approach (and vice-versa). EMSEC consequently considers formal methods for the verification of cryptographic protocols, and for performing risk assessments of real-life systems.

Formal proofs for cryptographic protocols. One extremely successful approach when designing and analyzing security protocols, is the use of formal methods. The purpose of formal verification is to provide rigorous frameworks and techniques to analyze protocols and find their flaws. In formal symbolic models, most of the cryptographic details are ignored using abstract structures, and the communication network is assumed to be entirely controlled by an omniscient attacker.

The complexity of the verification problem comes from the protocols themselves, as well as the need to clearly state the intended protocol goals and characterize the environment and the attacker capabilities. As experience with traditional protocols has shown, these are highly non-trivial tasks. Many protocols once believed to be secure

have been found to be flawed when formally modeled and analyzed. In the past three decades, remarkable advances have been made in the automated analysis of standard security protocols (e.g. for authentication and key exchange protocols), and nowadays several tools for protocol verification are available, e.g. Tamarin, and ProVerif.

We aim at extending these formal models and methods, and to develop new ones, to be able to analyze modern protocols. For instance, many modern protocols rely on a notion of state or time, and can not be analyzed using existing verification tools. Moreover, techniques to analyze privacy-type properties which are expressed relying on behavioral equivalences suffer from limitations and have not been studied as much as confidentiality and authentication properties.

Risk modeling and analysis. The objective of risk analysis is to decide how to protect the analyzed system in the best possible way. In order to reach this objective, possible attacks need to be identified and ranked, and the impact of the countermeasures to be implemented needs to be evaluated. The ultimate goal is to deploy countermeasures in such a way that the residual risks are acceptable.

Formal models are of great help while performing risk analysis. They allow to represent the analyzed system and its vulnerabilities in a rigorous way to enable their systematic qualitative and quantitative analysis. EMSEC investigates the use of attack trees and related models to support risk analysis. We are especially interested in formalizing the meaning of attack trees and their derivatives, their quantitative analysis, and their automated generation.

Cryptanalysis of block ciphers using solvers. As already mentioned in Section 2.2.1, formal methods, through the use of automatic tools like e.g. MILP and constraint programming solvers, are also used to do cryptanalysis of symmetric primitives, especially lightweight block symmetric ciphers.

2.2.3 Software / Hardware System Security

Side-channel attacks. The security of implementations is today quite a challenging problem as it leads to consider stronger adversaries than was thought before and more efficient attacks. For example, the best attack on AES in the black-box model can only attack 7 out of the 10 rounds, without hampering the security of this cipher, while without protections against side-channel attacks, it is possible to break it in practical time. In side-channel attacks, the attacker has access to additional information about intermediate variables and this leads to improved attacks. However we need to be able to recover this information either via external physical measurements via electro-magnetic probes or by exploiting micro-architectural components. EMSEC works on finding new side-channel attacks on embedded systems and on the design of secure implementations against these adversaries. We study in particular the resistance of lattice-based signature schemes proposed to the NIST post-quantum competition. We also propose a new tool for evaluating the security of masking schemes against different adversaries using formal methods. Furthermore, we study the security of PAKE implementations against cache attacks. In addition, we propose constant-time, or asynchronous, implementa-

tions for Gaussian sampling and WPA3 Dragonfly. It is worth noting that EMSEC follows the Responsible Disclosure practices when they identify serious vulnerabilities inside deployed components. We have recently collaborated with GlobalPlatform, FIDO Alliance, Google and Intel. Other industrial members, such as Facebook, ARM, and the Japanese NTT Data, have cooperated with us in order to mitigate our discovered flaws.

Micro-architectural attacks. EMSEC is widely recognized for developing attack techniques against implementations. It considers microarchitectural covert and side channels in commodity computers and servers, and in particular microarchitectural components that are shared between several processes, such as the CPU cache, DRAM and the branch prediction unit. To construct safe systems against microarchitectural attacks, we distinguish two main challenges: (1) as of today the real attack surface is unknown, both at the software level and at the hardware level, due to the lack of documentation of the hardware components and the lack of automated methods to analyze software; (2) proposed countermeasures are rarely adopted in practice, due to performance and security trade-offs. We aim to build automated methods to reverse engineer microarchitectural components and to detect vulnerabilities, as well as countermeasure that are practical and scale to real-world software.

Smartphone security The first smartphones were introduced in 2007 by Apple followed by Google in 2008, and since then, smartphones have become almost vital in the modern world. Consequently, nowadays, the stakes are high when it concerns the security of smartphones. Providers of smartphones systems have already anticipated this ongrowing need of security by integrating Trusted Execution Environments (TEE). The term TEE is often used to describe an isolated, secure integrity-protected execution environment, consisting of processing, memory and storage capabilities. This environment may run on the same computational hardware used by untrusted code, but the separation, unlike other approaches, is enforced through trustworthy hardware components. Trusted execution environments are fast becoming deployed in smartphones. Android, for instance, requires that a couple of its components to run inside a TEE. The most widely known examples of this are the Android KeyStore for cryptographic keys protection and Widevine for digital content management. Software running on the TEE can access device-specific keys required to decrypt secret keys. The main processor sees only the encrypted content, providing better security against various attacks. EMSEC studies the cryptographic implementations inside different trustlets (TEE applications). In addition, we work on automatic tools to study the different interfaces that exist between Android and the secure world.

3 Scientific achievements

Axis "Cryptography"

3.1 Symmetric Cryptography

Participants: Patrick Derbez, Stéphanie Delaune and Pierre-Alain Fouque.

Collaborations: LORIA (Nancy), EMN (Nantes).

In the ANR JCJC CryptAudit and ANR DECRYPT projects, the goal is to study the resistance of block ciphers and stream ciphers. We build new tools/models for automatically searching specific types of attacks or distinguishers.

In the recent project DECRYPT, we use Constrained Programming Tools for this task as they allow to represent the problem to solve more easily. In this project, we are also working with people in Nantes involved in the Choco CP solver and we investigate with them if we can improve their tool to solve cryptographic instances. A PhD student will be hired next year to work in this direction.

In the CryptAudit project, the task is the same but the approach is different as we mainly develop new ad-hoc tools to efficiently solve the problems Gurobi or Choco can not. One important application of these techniques is the search of integral distinguishers based on division property. We also generalized these attacks, showing they are not invariant by linear applications, and providing criteria to select the *good* linear combinations to look for. We also study the diffusion property of generalized Feistel, solving a 10-year open problem in this area at ToSC/FSE 2019. Finally, we won the third *SKINNY Challenge* as we found the most efficient practical attacks on lightweight block cipher SKINNY and this article has been accepted to SAC 2019.

3.2 Real-World Cryptography

Participants: Pierre-Alain Fouque, Céline Duguey, Angèle Bossuat, Adina Nedelcu and Raphaël Bost.

Collaborations: XLIM (Limoges), Bourges, Inria (Paris), Chalmers (Sweden), DGA (Rennes) and OrangeLabs (Rennes).

The security of real-world security protocols such as TLS and WhatsApp is an important problem. In the ANR SafeTLS project, with our partners we study these problems. We look at the security of TLS 1.3 and in particular the anonymity guarantees provided by the encryption as soon as possible mechanism of this protocol. This paper has been accepted at PoPETS 2019 with people from Orange Labs. We study the security of WhatsApp and we discover that there are some attacks, since an adversary

can for instance inject a message so that the legitimate user is no more authenticated. This result has been published at EuroSP 2019 with people from XLIM and Chalmers. We also propose a new mechanism when a user has multiple devices and wants to synchronize all his communications.

We continue our work on the security of database using symmetric searchable encryption scheme. We show that there is a tradeoff between the security of the scheme and their efficiency by proving some lower bound on the complexity of these schemes. This contribution has been published at PoPETS 2019.

3.3 Cryptanalysis of Public-Key Cryptography

Participants: Paul Kirchner, Pierre-Alain Fouque, Weiqiang Wen.

Collaborations: Thomas Espitau (Sorbonne University), Damien Stehlé (ENS Lyon), Martin Albrecht (RHUL), and Shi Bai (Florida University).

We extend the LLL algorithm for module lattices as such lattices are increasingly used in many post-quantum cryptosystems with Thomas Espitau and Paul Kirchner. We provide a very efficient implementation in gp which has been able to break very large dimensions between 1,000 and 10,000 with a high number of bits up to 1,000,000. This work has been accepted to CRYPTO 2020.

We have given an enumeration-based lattice reduction algorithm that runs in time $k^{0.125k}$ and achieves a root Hermite factor of $k^{1/(2k)}$. This improves on the previously best enumeration-based algorithms that run in time $k^{0.184k}$, while achieving the same quality. We note that these figure are for lattice reduction where the "block size" k is significantly smaller than the dimension d of the lattice.

The $k^{0.125k}$ time complexity has been speculated in previous work assuming the Geometric Series Assumption (GSA). To ensure that enumeration sees a GSA-like shape as input we propose to decouple the preprocessing context from the enumeration context. More precisely, the new algorithm preprocesses a projected sublattice of larger dimension than it aims to enumerate over. As a side effect, the dimension of the lattice is relatively large, compared to the block size.

To reduce the dimension requirement, we also describe a practical strategy, with enumeration beyond the GSA region, which works well in simulations/experiments for smaller dimensions. Our simulations and experiments indicate it achieves the above claimed complexity for cryptographic sizes and $d \approx 2k$.

On cryptographic impacts, lattice sieving algorithms still outperform the lattice enumeration of this work for manageable parameters. Nevertheless we hope our approach can be helpful in assessing enumeration-like, memory efficient algorithms. This paper has been accepted at CRYPTO 2020.

3.4 Lattice-based cryptography: security foundations

Participants: Katharina Boudgoust, Adeline Roux-Langlois, Weiqiang Wen.

Collaborations: Shi Bai (Florida Atlantic University).

We studied the hardness of fundamental problems used in lattice-based cryptography. Today, most of those constructions are based on the Learning With Errors (LWE) problem, and are secure under the hardness of this problem which is shown to be hard using worst-case to average-case reduction from hard problem on lattices To gain in efficiency, the approach used is to consider structured version of LWE such as Polynomial/Ring LWE, Module LWE or Middle-Product LWE. Even if those variants also benefits worst-case to average-case reductions from lattices problems, we have no guarantee that those structured lattices should be at least as hard as the general ones.

In a first work, we introduced the *Middle-Product Computational Learning With Rounding* problem, which is an adaptation of the computational LWR problem over rings (used to derandomize LWE type encryption.). We proved that this new assumption is as hard as the decisional version of MP-LWE and thus benefits from worst-case to average-case hardness guarantees[BBD+19].

In a second work, we studied the hardness of Module-LWE with binary secret. The binary secret variant of LWE (bin-LWE) is widely-used version of the problem, where the secret vector s is chosen from $\{0,1\}^n$. Besides gaining in efficiency, this variant also plays an important role in some applications like fully homomorphic encryption schemes. Several results already studied the hardness of bin-LWE, but none of them is easy to adapt to structured variant like Ring or Module-LWE. Finally, having this result also allow to give a classical reduction from hard problem on lattice to Module-LWE, for some particular parameters.

3.5 Lattice-based cryptography: advanced signature schemes

Participants: Pauline Bert, Gautier Eberhart, Adela Georgescu, Guillaume Kaim, Adeline Roux-Langlois, Mohamed Sabt.

Collaborations: Sébastien Canard, Jacques Traoré (Orange Labs, Caen).

In a first work, we developed and implemented efficient Gaussian preimage sampling techniques on module lattices, which rely on the works of Micciancio and Peikert in 2012, and Micciancio and Genise in 2018. The main advantage of our implementation is its modularity, which makes it practical to use for signature schemes, but also for more advanced constructions using trapdoors. In particular, it is easy to use in the ring or module setting, and to modify the arithmetic on Rq (as different schemes have different conditions on q). Relying on these tools, we also presented two instantiations and implementations of proven trapdoor-based signature schemes in the module setting: GPV in the random oracle model and a variant of it in the standard model.

In a second work, we studied the problem of Gaussian sampling over integers. Our main concerns were threefold: efficiency, resistance against side-channel attacks and universality with respect to Gaussian parameters. We addressed this problem by analyzing

[BBD+19] S. Bai, K. Boudgoust, D. Das, A. Roux-Langlois, W. Wen, Z. Zhang, "Middle-Product Learning with Rounding Problem and Its Applications", *in: ASIACRYPT (1)*, *Lecture Notes in Computer Science, 11921*, Springer, p. 55–81, 2019.

the rejection-based algorithm of Karney. We showed that this algorithm is vulnerable to timing attack and we used this to compromise the PALISADE implementations of some schemes. Then, we designed a strictly constant-time Gaussian sampler and implemented using SIMD AVX512. Our algorithm does not contain any branch or loop, thereby avoiding state-of-the-art cache attacks.

In a third work, in collaboration with Orange Labs, we build a blind signature and its partially blind variant based on lattices assumptions. Blind signature is a cornerstone in privacy-oriented cryptography and we propose the first lattice based scheme without restart. Compare to related work, the key idea of our construction is to provide a trapdoor to the signer in order to let him perform some gaussian pre-sampling during the signature generation process, preventing this way to restart from scratch the whole protocol. We prove the security of our scheme under the ring k-SIS assumption, in the random oracle model. Finally, we provided a full implementation of our scheme.

Finally, we also worked on group signature schemes. Group signatures were designed to allow only members of a group to sign messages while the identity of the signer remains hidden for the verifier (anonymity). The latter can only ensure that a member belonging to the group has signed the message, moreover this property guarantees the unlinkability as well, preventing anyone to detect that two group signatures have been generated by the same group member. Nevertheless, if necessary, the signature can be opened by an entity called group manager who holds some secret information and reveals the identity of the signer (traceability). These features make group signatures very useful for real life applications including e-commerce systems, anonymous online communications and trusted hardware attestations.

3.6 Lattice-based cryptography: NTRU encryption scheme

Participants: Pierre-Alain Fouque, Paul Kirchner, Yang Yu.

Pierre-Alain, Paul and Yang work on a new version for NTRU encryption scheme. This scheme is more compact and the performance are very good. This scheme uses the same key as in Falcon. This work is currently in submission.

3.7 Secure Tunnels for Constrained Environments

Participants: Gildas Avoine, Loïc Ferreira.

Collaborations: Sébastien Canard, Orange Labs, Caen.

The objective of this collaborative work is to analyze and design lightweight cryptographic primitives and protocols for the Internet of Things. In particular, we aim to design a protocol to allow two connected parties to establish secure channels, typically between a server and a smartcard. Such a channel should take the capacities into account, in terms of computation, communication, and storage. For that, we analyzed existing solutions and found weaknesses in Lorawan 1.0[AF18b] and SCP02[AF18a]. The

[AF18b] G. Avoine, L. Ferreira, "Rescuing LoRaWAN 1.0", *in: Financial Cryptography and*

design of a new protocol with the matching security model is in progress.

3.8 Distance Bounding Protocol Design

Participants: Gildas Avoine, Olivier Gimenez.

Collaborations: Jacques Traoré, Orange Labs Caen.

A *mafia fraud* is a man-in-the-middle attack applied against an authentication protocol where the adversary simply relays the exchanges without neither manipulating nor understanding them. The earliest version of this attack was introduced by Conway in 1976 and is known as the *chess grandmaster problem*. In this problem, a little girl is able to compete with two chess grandmasters during a postal chess game, where she transparently relays the moves between the two grandmasters. She eventually wins a game or draws both. In modern cryptography, mafia frauds can typically be used against authentication protocols. The adversary relays the messages between the prover and the verifier, who think they communicate together, while there is an adversary in the middle. This so-called mafia fraud was actually suggested by Desmedt, Bengio and Goutier in 1987 to defeat the Fiat-Shamir protocol. Brands and Chaum proposed in 1994 a *distance-bounding protocol* that aims to thwart mafia fraud. The distance estimation relies on the measurement of the Round-Trip-Time (RTT) of single bit exchanges between the verifier and the prover. Considering the physical impossibility to travel faster than the speed of light, RTT bounds the distance between the parties. EMSEC designed distance bounding protocols for contactless devices[ABG+17,ABK+11]. We now also consider distance bounding protocols to detect malicious traffic diversion on Internet.

3.9 Time-Memory Trade-Off (TMTO)

Participants: Gildas Avoine, Barbara Fila, Diane Leblanc-Albarel, Florent Tardif.

Collaborations: Xavier Carpent (KULeuven, Belgium).

A cryptanalytic time-memory trade-off (TMTO) is a technique introduced by Martin Hellman in 1980 to reduce the time needed to perform an exhaustive search. The key-point of the technique resides in the precomputation of tables that are then used to speed up the attack itself. Given that the precomputation phase is much more

Data Security: 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 2018, `https://hal.archives-ouvertes.fr/hal-02182929`.

[AF18a] G. Avoine, L. Ferreira, "Attacking GlobalPlatform SCP02-compliant Smart Cards Using a Padding Oracle Attack", *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018, `https://hal.archives-ouvertes.fr/hal-02182927`.

[ABG+17] G. Avoine, D. Bultel, S. Gambs, D. Gérault, P. Lafourcade, C. Onete, J.-M. Robert, "A Terrorist-fraud Resistant and Extractor-free Anonymous Distance-bounding Protocol", *in: Asia Conference on Computer and Communications Security – ASIACCS'17*, ACM, p. To Appear, Abu Dhabi, UAE, April 2017.

[ABK+11] G. Avoine, M. A. Bingöl, S. Kardaş, C. Lauradoux, B. Martin, "A Framework for Analyzing RFID Distance Bounding Protocols", *Journal of Computer Security – Special Issue on RFID System Security 19*, 2, March 2011, p. 289–317.

expensive than an exhaustive search, a TMTO makes sense in a few scenarios, e.g., when the adversary has plenty of time for preparing the attack while she has a very little time to perform it, the adversary must repeat the attack many times, or the adversary is not powerful enough to carry out an exhaustive search but she can download precomputed tables. Problems targeted by TMTOs mostly consist in retrieving the preimage of a hashed value or, similarly, recovering a cryptographic key through a chosen plaintext attack. EMSEC collaborates with KULeuven (Belgium) on TMTO techniques[AC17][ACL15][TACK17]. We aim to provide improvements on the techniques to build and store tables, and we also consider practical issues, for example the benefit of using an SSD instead of RAM, and the distribution of the precomputation.

3.10 Security of Cryptographic Implementations

Participants: Daniel De Almeida Braga, Pierre-Alain Fouque, Mohamed Sabt.

GlobalPlatform (GP) card specifications are defined for smart cards regarding rigorous security requirements. The increasingly more powerful cards within an open ecosystem of multiple players stipulate that asymmetric-key protocols become necessary. We analyze SCP10, which is the Secure Channel Protocol (SCP) that relies on RSA for key exchange and authentication. Our findings are twofold. First, we demonstrate several flaws in the design of SCP10. We discuss the scope of the identified flaws by presenting several attack scenarios in which a malicious attacker can recover all the messages protected by SCP10. We provide a full implementation of these attacks. For instance, an attacker can get the freshly generated session keys in less than three hours. Second, we propose a secure implementation of SCP10 and discuss how it can mitigate the discovered flaws. Finally, we measure the overhead incurred by the implemented countermeasures.

This paper has been accepted at CHES 2020 [BFS20]. Moreover, the paper has incited GlobalPlatform to collaborate with us in order to write a new version of the standard by taking our recommendations into consideration.

[AC17] G. Avoine, X. Carpent, "Heterogeneous Rainbow Table Widths Provide Faster Cryptanalyses", *in: Asia Conference on Computer and Communications Security – ASIACCS'17*, ACM, p. To Appear, Abu Dhabi, UAE, April 2017.

[ACL15] G. Avoine, X. Carpent, C. Lauradoux, "Interleaving Cryptanalytic Time-Memory Trade-Offs on Non-uniform Distributions", *in: European Symposium on Research in Computer Security – ESORICS*, G. Pernul, P. Y. A. Ryan, E. R. Weippl (editors), *Lecture Notes in Computer Science*, *9326*, Springer-Verlag, p. 165–184, Vienna, Austria, September 2015.

[TACK17] F. TARDIF, G. Avoine, X. Carpent, B. Kordy, "How to Handle Rainbow Tables with External Memory", *in: Australasian Conference on Information Security and Privacy*, P. J., S. S. (editors), *ACISP 2017: Information Security and Privacy*, *10342*, Part I, Paul Watters and Julian Jang-Jaccard, p. pp 306–323, Auckland, New Zealand, July 2017, `https://hal.archives-ouvertes.fr/hal-01563841`.

[BFS20] D. D. A. Braga, P. Fouque, M. Sabt, "The Long and Winding Path to Secure Implementation of GlobalPlatform SCP10", *in: CHES*, p. 96–218, 2020.

Axis "Formal Methods for Security"

3.11 Symbolic analysis of distance bounding protocols

Participants: Alexandre Debant, Stéphanie Delaune, Cyrille Wiedling.

Collaborations: Ioana Boureanu (University of Surrey), Tom Chothia (University of Birmingham).

The research community in logics, program verification, and security has already a long tradition in developing techniques and tools to analyse key establishment and authentication protocols. However, distance bounding protocols which are used to provide secure proximity control, raise new research challenges, and can not be analysed today using off-the-shelf symbolic verification tools (e.g., ProVerif). To fill this gap, we have developed novel techniques to automatically analyse distance bounding protocol within the symbolic framework.

We proposed a formal definition of terrorist fraud resistance and several reduction results: when looking for an attack, it is actually sufficient to consider a simple scenario involving at most four participants located at some specific locations. Moreover, actually, we can consider a particular strategy when looking for a terrorist fraud attack. These reduction results allow one to use verification tools (e.g., ProVerif, Tamarin) developed for analysing more classical security properties [DDW19]. We have also developed a new procedure for analysing a bounded number of sessions of distance bounding protocols. This procedure has been integrated in the AKISS verification tool [DD19]. As an application, we analyse severl distance bounding protocols, as well as some contactless payment protocols.

We are working on an extension of this result to consider contactless payment protocols for which the verifier (i.e. the terminal) is not supposed to behave honestly, and we also want to consider richer scenario in which mobility of the agents are taken into account.

3.12 Deciding equivalence-based properties in the bounded setting

Participants: Antoine Dallon, Stéphanie Delaune, Joshua Peignier.

[DDW19] A. Debant, S. Delaune, C. Wiedling, "Symbolic Analysis of Terrorist Fraud Resistance", *in : Computer Security - ESORICS 2019 - 24th European Symposium on Research in Computer Security, Luxembourg, September 23-27, 2019, Proceedings, Part I*, p. 383–403, 2019, https://doi.org/10.1007/978-3-030-29959-0_19.

[DD19] A. Debant, S. Delaune, "Symbolic Verification of Distance Bounding Protocols", *in : Principles of Security and Trust - 8th International Conference, POST 2019, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2019, Prague, Czech Republic, April 6-11, 2019, Proceedings*, p. 149–174, 2019, https://doi.org/10.1007/978-3-030-17138-4_7.

Collaborations: Véronique Cortier (LORIA).

In the symbolic setting, privacy-type properties are often expressed an equivalences. The problem of deciding whether an equivalence, expressing a privacy property, holds or not is well-known to undecidable in general. Therefore, we aim at designing decision procedures in a restricted setting: the bounded setting. This allows us to obtain security guarantees when the protocol is executed a bounded number of times. Analysing n sessions of a protocol does not allow in general to derive security guarantees when the protocol is executed one more time, but this allows us to gain confidence on the security of the protocol.

We developed our own decision procedure based on graph planning and SAT solving. This decision procedure is based on a typing result: if there is an attack then there is a "small" one which only involves messages having specific types.The decision procedure has been first designed for symmetric primitives [CDD17], and then extended to the case of asymetric primitives (e.g. asymetric encryption, and signature) [CDD18]. This procedure has been implemented in the tool Sat-Equiv. We are currently working on an extension of this procedure to be able to consider protocols that feature else branches.

3.13 Establishing equivalence-based properties in the general case

Participants: Stéphanie Delaune, Solène Moreau, Vaishnavi Sundararajan.

Collaborations: David Baelde (ENS Paris Saclay), Véronique Cortier (LORIA).

Existing tools and techniques do not allow to verify directly privacy-type properties, expressed as behavioral equivalences in the unbounded setting. We proposed a different approach: we designed sufficient conditions on protocols which are sufficient to ensure anonymity and unlinkability, and which can then be effectively checked automatically using ProVerif. Our two conditions correspond to two broad classes of attacks on unlinkability, i.e. data and control-flow leaks. This theoretical result is general enough that it applies to a wide class of protocols based on a variety of cryptographic primitives. In particular, using our tool, UKano, we provide the first formal security proofs of protocols such as BAC and PACE (e-passport), Hash-Lock (RFID authentication), etc. Our work has also lead to the discovery of new attacks, including one on the LAK protocol (RFID authentication) which was previously claimed to be unlinkable (in a weak sense) [HBD19]. We are currently working to extend this result to the case of stateful protocols.

[CDD17] V. Cortier, A. Dallon, S. Delaune, "SAT-Equiv: An Efficient Tool for Equivalence Properties", *in: CSF 2017 - 30th IEEE Computer Security Foundations Symposium*, IEEE, Santa Barbara, France, August 2017, https://hal.archives-ouvertes.fr/hal-01906641.

[CDD18] V. Cortier, A. Dallon, S. Delaune, "Efficiently deciding equivalence for standard primitives and phases", *in: ESORICS 2018 - 23rd European Symposium on Research in Computer Security*, Barcelona, Spain, September 2018, https://hal.inria.fr/hal-01900083.

[HBD19] L. Hirschi, D. Baelde, S. Delaune, "A method for unbounded verification of privacy-type properties", *J. Comput. Secur. 27*, 3, 2019, p. 277–342, https://doi.org/10.3233/JCS-171070.

We are also currently working (with V. Sundararajan and V. Cortier) to identify a class of protocols for which trace equivalence is decidable in the general setting (i.e., for an unbounded number of sessions and unlimited fresh nonces). The class we have identified encompasses most symmetric and asymetric key exchange protocols of the literature, in their tagged variant.

3.14 Security Modeling with Attack–Defense Trees

Participants: Barbara Fila, Wojciech Wideł.

Risk analysis is a very complex process. It requires rigorous representation and in-depth assessment of threats and countermeasures. We focus on the formal modeling of security issues using attack–defense trees, see Figure 1. These are used to represent and quantify potential attacks in order to better understand the security issues that the analyzed system may face. They therefore make it possible to guide an expert in the choice of countermeasures to be implemented to secure their system.

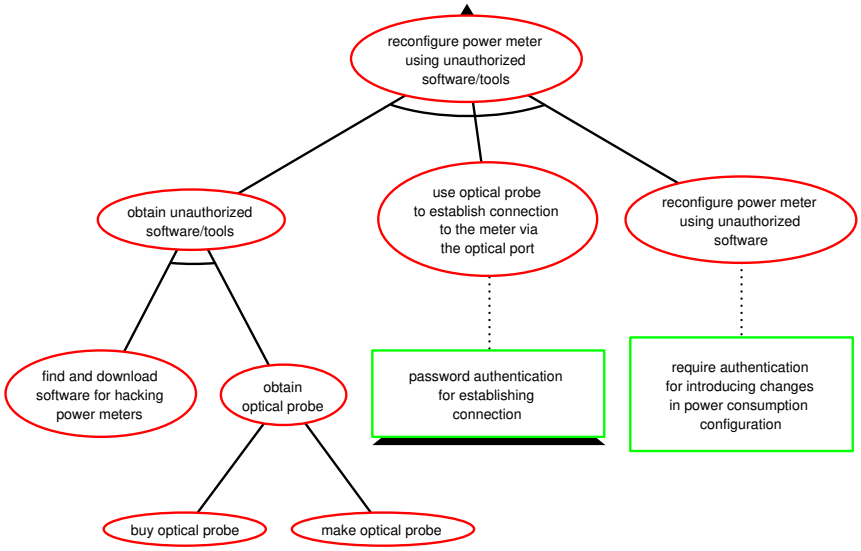


Figure 1: Attack–defense tree for abusing power meter[FW19a]

In 2019, we focused on practical aspects of attack–defense trees:

- The cheapest attacks are often time-consuming, and those requiring high level of technical skills might occur rarely but result in disastrous consequences. Therefore, analysis focusing on a single parameter at a time, e.g., only cost or time, is insufficient for the successful selection of the appropriate measures increasing system's security. In practice, security engineers are thus confronted with the problem of multi-parameter analysis. We addressed this problem in [FW19b], where we

[FW19b] B. Fila, W. Widel, "Efficient Attack–Defense Tree Analysis using Pareto Attribute Domains", *in: 2019 IEEE 32nd Computer Security Foundations Symposium (CSF)*, IEEE,

proposed a general framework based on Pareto optimality, and allowing for quantitative analysis of security taking several criteria, such as cost, time, probability, difficulty, etc. into account.

- In most existing approaches, an attack tree represents generic ways of attacking a system, but without taking any specific system or its configuration into account. This means that such a generic attack tree may contain attacks that are not applicable to the analyzed system, and also that a given system could enable some attacks that the attack tree did not capture. To overcome this problem, we extend the attack tree setting with a model of the analyzed system, allowing us to introduce precise path semantics of an attack tree and to define the concept of missing attacks[PFWTM19].

- We performed a real-life case study where we used attack–defense trees to analyze how to tamper with optical power meter to record lower than the actual electricity consumption has been performed and described[FW19a]. We took various quantitative aspects into account, in order to identify optimal strategies for customers trying to lower their electricity bills, and for electricity providers aiming at securing their infrastructures from thefts. This case study allowed us to validate the previously developed methods for quantitative analysis of attack–defense trees.

- To facilitate the usage of attack–defense trees in practice, we have implemented a tool called OSEAD (*Optimal Strategies Extractor for Attack–Defense trees*)[FW19a]. The tool automates resolution of various optimization problems on attack–defense trees, in particular finding optimal attacks with respect to a single parameter[KW18], finding Pareto optimal attacks[FW19b], and finding an optimal set of countermeasures[FW20].

- During the last half decade, the security modeling community witnessed a growing interest in employing formal methods to deal with the problem of constructing and analyzing attack trees and related models. To ensure the existing knowledge transfer, we survey recent advances in graphical security modeling with focus on the

---

p. 200–215, Hoboken, United States, June 2019, `https://hal.archives-ouvertes.fr/hal-02308407`.

[PFWTM19] S. Pinchinat, B. Fila, f. F. Wacheux, Y. Thierry-Mieg, "Attack Trees: A Notion of Missing Attacks", *in: GraMSec 2019 - 6th International Workshop on Graphical Models for Security, Lecture Notes in Computer Science, 11720*, p. 23–49, Hoboken, NJ, United States, June 2019, `https://hal.archives-ouvertes.fr/hal-02533750`.

[FW19a] B. Fila, W. Widel, "Attack–Defense Trees for Abusing Optical Power Meters: A Case Study and the OSEAD Tool Experience Report", *in: GraMSec@CSF, LNCS, 11720*, Springer, p. 95–125, 2019.

[KW18] B. Kordy, W. Widel, "On Quantitative Analysis of Attack–Defense Trees with Repeated Labels", *in: POST, Lecture Notes in Computer Science, 10804*, Springer, p. 325–346, 2018.

[FW19b] B. Fila, W. Widel, "Efficient Attack–Defense Tree Analysis using Pareto Attribute Domains", *in: 2019 IEEE 32nd Computer Security Foundations Symposium (CSF)*, IEEE, p. 200–215, Hoboken, United States, June 2019, `https://hal.archives-ouvertes.fr/hal-02308407`.

[FW20] B. Fila, W. Widel, "Exploiting attack–defense trees to find an optimal set of countermeasures", *in: 2020 IEEE 33rd Computer Security Foundations Symposium (CSF)*, IEEE, 2020.

application of formal methods to the interpretation, (semi-)automated creation, and quantitative analysis of attack trees and their extensions, in [WAFP19]. The objective of this work is to provide a unified description of existing frameworks, compare their features, and outline interesting open questions.

On December 3, 2019, Wojciech Wideł defended his thesis titled *Formal modeling and quantitative analysis of security using attack–defense trees.*

[WAFP19] W. Widel, M. Audinot, B. Fila, S. Pinchinat, "Beyond 2014: Formal Methods for Attack Tree-based Security Modeling", *ACM Computing Surveys 52*, 4, September 2019, p. 1–36, `https://hal.archives-ouvertes.fr/hal-02308427`.

Axis "Hardware and Software Systems Security"

3.15 Side-Channel Attacks

Participants: Benoît Gérard, Pierre-Alain Fouque, Paul Kirchner, and Yang Yu.

Collaborations: Mehdi Tibouchi (NTT Japan), Thomas Espitau (Sorbonne University), Gilles Barthe (IMDEA, MPI Bochum), Benjamin Grégoire (Inria Sophia-Antipolis), Mélissa Rossi (Thalès/ANSSI/ENS), Sonia Belaïd (CryptoExperts), François-Xavier Standaert (UCL).

In this area we construct tools for verifying the security of implementation against hardware attacks and we propose attacks and secure implementations for lattice-based schemes proposed for instance at the NIST competition.

At ESORICS 2019, we propose a tool for verifying the security of hardware implementations against stronger attacks called glitch effect. Glitch effect is a physical mechanism that gives more information to the adversary. In hardware, the signal in each wire does not propagate at the same speed. If a 0 arrives at an AND gate, the output of the gate can be computed and the 0 signal is output regardless of the second wire. In this scenario, the adversary can recover from one measurement at the end of the gate the value of one input wire. Usually this phenomenon is not allowed to the adversary: he has to probe a wire if he wants to know its value, while here from one measurement (at the output wire), he is able to know 2 wires. Similar bad cases can happen for other gates such as the OR gate. For example, it has been shown that even if a circuit is protected using masking randomization, if glitches happen, the security of the circuit can be annihilated. We modify our tool to automatically look at the security of masking scheme using such stronger adversaries.

At ACNS 2019, we evaluate a masked implementation on the Dilithium signature scheme, which is a candidate to the NIST post-quantum competition organized by the NIST with Vincent Migliore (postdoc in 2018) and Benoît Gérard. This work follows our previous EUROCRYPT 2018 paper which describes the masking technique we have to use. Here, we look at the security of the signature scheme. Without any masking, the scheme can be attacked. Then, we apply our transformation and we show that the signal/noise is too weak for the adversary. This work took time because during the experimentation, we use a Cortex M3 processor. We first use simulation to predict the value using an automatic tool. When we go to the board, the simulation were not correct with our experiments. We have a specific leakage. In order to understand the leakage, we discovered that the layout of this processor was public and from the hardware circuit, we were able to explain the leakage difference. By adding a flip-flop in the desing, we were able to cancel this bad effect.

At CCS 2019 we use a machine learning algorithm, called phase retrieval algorithms, to break the lattice-based BLISS signature scheme. We show that we can exploit a tiny

leakage and this powerful statistical tool allows to recover the secret-key. Then, we propose a new method to secure the use of transcendental function using a clever use of lattice reduction in Sobolev space by approximating such functions with polynomials. Contrary to previous tool to approximate these functions, which introduces some poor approximations in the method, our method avoids this effect.

With Yang Yu, Paul Kirchner and Mehdi Tibouchi we also look at the security of the DLP and Falcon signature schemes. In a nutshell, we show that the Gram-Schmidt norms of the NTRU secret basis reveals the secret basis. We mount a real attack on the DLP scheme. For Falcon, the attack is harder and we devise another attack. Falcon is another lattice-based signature scheme, proposed at the NIST post-quantum competition. The result of this paper has been accepted at EUROCRYPT 2020. Following the discovery of this attack, the authors of Falcon proposed a new constant-time implementation, meaning that the signing time does not depend on the secret.

3.16 Micro-architectural attacks

Participants: Clémentine Maurice.

Collaborations: Daniel Gruss (TU Graz, Austria), Michael Schwarz (TU Graz, Austria), Moritz Lipp (TU Graz, Austria), Vedad Hadzic (TU Graz, Austria), Arthur Perais (Microsoft, USA), Sarani Bhattacharya (KU Leuven, Belgium), Shivam Bhasin (NTU Singapore), Debdeep Mukhopadhyay (IIT Kharagpur, India).

One major obstacle to a thorough analysis of the attack surface on hardware is the lack of documentation of micro-architectural components by vendors. While performing side-channel attacks, by construction and considering our hypotheses, we never directly observe what we seek to measure. We, therefore, rely on our knowledge of the environment for accurate indirect measurements, as well as for effective countermeasures. To address this issue, we worked on the reverse-engineering of specific micro-architectural components.

First, we reverse-engineered a part of the Branch Prediction Unit of Intel CPUs. This work, in collaboration with S. Bhattacharya, S. Bhasin and D. Mukhopadhyay led to more precise side-channel attacks on the branch predictor [BMBM20].

Second, we reverse-engineered the way predictor of AMD CPUs, in collaboration with A. Perais and the CoreSec team of TU Graz (D. Gruss, M. Schwarz, M. Lipp and V. Hadzic). Cache way predictors were introduced by AMD as an energy consumption and performance optimization. We reverse-engineered AMD's L1D cache way predictor in micro-architectures from 2011 to 2019, resulting in two new attack techniques dubbed Collide+Probe and Load+Reload. We demonstrated that this side channel can be used in a covert channel up to 588.9 kB/s, in side-channel attacks against vulnerable cryptographic implementations, and reducing the entropy of the ASLR of the kernel of

[BMBM20] S. Bhattacharya, C. Maurice, S. Bhasin, D. Mukhopadhyay, "Branch Prediction Attack on Blinded Scalar Multiplication", *IEEE Trans. Computers 69*, 5, 2020, p. 633–648.

a fully patched Linux system [LHS+20].

3.17 Data re-identification

Participants: Gildas Avoine.

Collaborations: Antonin Voyez (Druid team), Tristan Allard (Druid team), Elisa Fromont (Lacodam team).

We work on the re-identication of time series data, especially data issued by smart meters. We develop attacks to re-identify existing data, and we also improve the current anonymisation techniques. We also consider other applications, for example the anonymisation of public transportation data.

3.18 Security of Real-World Authentication Systems

Participants: Gwendal Patat, Mohamed Sabt.

Supported by leading web service providers, the FIDO Alliance defines the Universal 2nd Factor (U2F) protocols, an industrial standard that proposes a challenge-response 2FA solution. The U2F protocols have been thoughtfully designed to ensure high security. Although much attention was paid to make U2F easy to use, many users express inconvenience because of the repeated extra step that it would take to log in. In order to address this, several service providers offer a remember me feature that removes the need for 2FA login on trusted devices. We present the first systematic analysis of this undocumented feature, and we show that its security implications are not well understood. After introducing the corresponding threat models, we provide an experimental study of existing implementations of remember me. Here, we consider all the supporting websites considered by Yubico. The findings are worrisome: our analyses indicate how bad implementations can make U2F solutions vulnerable to multiple attacks. Moreover, we show that existing implementations do not correspond to the initial security analysis provided by U2F. We also implement two attacks using the identified design flaws. Finally, we discuss several countermeasures that make the remember me feature more secure.

This paper has been presented at SSTIC 2020 and it is still in submission for other international venues. Moreover, our two presentations at FIC 2020 and SSTIC 2020 have incited FIDO Alliance to start a recent collaboration with us in order to force the service providers to take our recommendations into consideration.

[LHS+20] M. Lipp, V. Hadzic, M. Schwarz, A. Perais, C. Maurice, D. Gruss., "Take A Way: Exploring the Security Implications of AMD's Cache Way Predictors", *in: Proceedings of the 15th ACM ASIA Conference on Computer and Communications Security (ASIACCS'20)*, 2020.

4 Software development and platforms

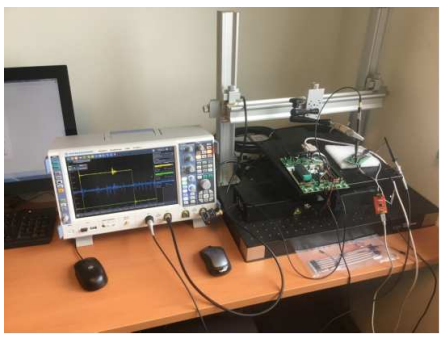
4.1 Platform "Cryptographic Computing" (PF-SP3-02)

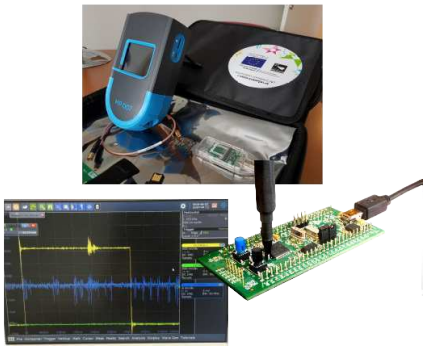
The platform PF-SP3-02 has a large computing capacity as well as a large memory capacity both in terms of storage memory and fast-access memory (RAM/SSD). The platform so consists of a 128-core computer and a 64-core computer, both benefiting from a 1-TB RAM. The plateform will be completed in 2020 with a computer hosting two EPYC 7H12 processors (64 cores / processor) and 1-TB RAM.

Due to its high-capacity, the platform allows the team to perform heavy computations, especially attacks on symmetric-key cryptographic algorithms, including cryptanalytic time-memory trade-offs. The platform is hosted in the data center of INSA Rennes (http://www.insa-rennes.fr/plateau-informatique.html). It has been funded by the project CPER SSI (FEDER, Région Bretagne, Rennes Métropole).

4.2 Platform "Attacks on Embedded Systems" (PF-SP3-01)

The platform PF-SP3-01 consists of an oscilloscope and probes, as well as an ISO14443 and ISO15693 protocol analyzer for contactless devices. It is jointly managed by Université Rennes 1 and INSA Rennes, and it is located at IRISA. In 2019, the platform was completed with a Faraday cage and a Cellebrite device to extract data from embedded devices. The main objective of this platform is to verify that the security of cryptographic protocols or algorithms is not weakened by their implementation. The platform allows the team to perform attacks on embedded systems, typically smart cards. The platform covers systems using radio frequency communications (RFID). The attacks are then at the level of the communication protocols by listening or injecting packets in the communication. In particular, it makes it possible to take precise time measurements to analyze the resistance of authentication distance-bounding protocols. The platform also allows the team to perform physical attacks, e.g., faults attacks. The platform can so test attacks against real implementations, but it can also test countermeasures, including whether they limit the amount of information an adversary can obtain.





5 Contracts and collaborations

5.1 International Initiatives

5.1.1 ERC POPSTAR

- Funding: H2020 ERC
- Hosting Institution: CNRS
- Budget: 1 500 000 EUR
- PI: Stéphanie Delaune
- Period: 02/17 - 01/22
- URL: `https://popstar.irisa.fr`
- Description: The main objective of the POPSTAR project is to develop foundations and practical tools to analyze modern security protocols that establish and rely on physical properties. The POPSTAR project will significantly advance the use of formal verification to contribute to the security analysis of protocols that rely on physical properties. This project is bold and ambitious, and answers the forthcoming expectation from consumers and citizens for high level of trust and confidence about contactless nomadic devices.

5.1.2 PROMETHEUS

- Funding: H2020
- Hosting Institution: UR1
- Budget: 520 000 EUR
- PI: Benoît Libert (ENS Lyon)
- EMSEC: Pierre-Alain, Adeline, Mohamed, Weiqiang, Gautier - UR1 is the leader of Workpackage 4 and Adeline is the Dissemination manager of the project
- Period: 01/01/2018 - 31/12/2022
- URL: `http://prometheuscrypt.gforge.inria.fr/`
- Description: PROMETHEUS is a Horizon 2020 project funded for four years by the European Union (under grant agreement No 780701). The project gathers twelve partners from seven countries: seven of the partners are universities and/or research institutes, one is a SME partner and four are industrials. PROMETHEUS aims to provide post-quantum signature schemes, encryption schemes and privacy-preserving protocols relying on lattice.

5.2 National Initiatives

5.2.1 ANR SafeTLS

- Funding: ANR
- Hosting Institution: UR1
- Budget total : 500 000 EUR
- PI: Pierre-Alain Fouque
- Period: 2016 - 2020
- URL: `http://safetls.gforge.inria.fr/`
- Description: The goal of this ANR project is to study the security of the new TLS 1.3 protocol that will be released in April 2017. We look at the security in various case studies such as Keyless SSL, MC-TLS, reverse-firewall and the security of implementations with our partners in Inria Sophia-Antipolis, Inria Paris, ANSSI, INSA. Indeed, since all internet communications will be encrypted in 2/3 years, new functionalities have to be designed or taken into account with TLS.

5.2.2 ANR TECAP

- Funding: ANR
- Hosting Institution: CNRS
- Budget EMSEC: About 15 000 EUR
- PI: Vincent Cheval (LORIA)
- EMSEC: Stéphanie (PI local)
- Period: 2018 - 2022
- URL: `http://anr17-tecap.gforge.inria.fr/`
- Description: Formal methods have been shown successful in proving security of cryptographic protocols and finding flaws. However manually proving the security of cryptographic protocols is hard and error-prone. Hence, a large variety of automated verification tools have been developed to prove or find attacks on protocols. These tools differ in their scope, degree of automation and attacker models. Despite the large number of automated verification tools, several cryptographic protocols still represent a real challenge for these tools and reveal their limitations. The aim of this project is to get the best of all these tools, meaning, on the one hand, to improve the theory and implementations of each individual tool towards the strengths of the others and, on the other hand, build bridges that allow the cooperations of the methods/tools.

5.2.3 ANR Decrypt

- Funding: ANR
- Hosting Institution: UR1
- Budget EMSEC:
- PI: Marine Minier (LORIA)
- EMSEC: Patrick (PI local), Stéphanie, Pierre-Alain
- Period: 2019 - 2023
- URL: `https://decrypt.limos.fr`
- Description: Cryptography is a cornerstone of everyday digital security as it aims at ensuring confidentiality and integrity of digital communications. These tasks are achieved by using keys (i.e., strings of characters) to encrypt and decrypt messages. In symmetric cryptography, the same key is used both to encrypt and decrypt messages, whereas in public key (asymmetric) cryptography, a public key is used for encryption and a different private key is used for decryption. In applications such as e-commerce or bank transactions, hybrid cryptography combines both forms of cryptography to create a secure channel: first, public key cryptography is used to cipher a common key; then symmetric cryptography is used to encrypt and decrypt transactions with the common key, mostly because it is faster. In this project, we focus on symmetric cryptography which is widely used.

5.2.4 ANR MobiS5

- Funding: ANR
- Hosting Institution: UR1
- Budget total: 637 878 EUR
- Budget EMSEC: 35 500 EUR
- PI: Cristina Onete (Limoges)
- EMSEC: Pierre-Alain et Clémentine
- Period: 01/09/2019 - 31/03/2024
- URL: `https://mobis5.limos.fr/index.html`
- Description: For 20 years, 3G and 4G mobile networks have allowed users to receive service anywhere, at any time. The dawning, visionary 5th generation mobile network (5G) aims to make telecommunications ubiquitous by using a decentralized architecture, including a massive Internet of Things (mIoT) and a non-federated core network. An important difference between current and future

mobile architectures is the variety of devices for which security solutions must be found. Current mobile phones are vulnerable to many attacks, such as malware, Denial-of-Service (DoS), tracking, and cryptographic attacks. Future networks will include IoT devices, which are even more attack-prone, and can be used as "tools" in cyber-attacks. The transition to 5G networks is expected to not only combine, but to compound risks to all types of devices.

MobiS5 aims to counter security threats in 5G architectures by providing a provably-secure cryptographic toolbox for 5G networks, validated formally and experimentally, addressing 5G architectures at 3 levels: (1) Infrastructure and physical end-point security, (2) Cryptographic primitives and protocols, (3) Mobile applications.

5.2.5 ANR ARCHI-SEC

- Funding: ANR
- Hosting Institution: CNRS
- Budget total: 707 417 EUR
- Budget EMSEC: 136 617 EUR
- PI: Jean-Luc Danger (Telecom ParisTech)
- EMSEC: Clémentine (local PI)
- Period: 01/10/2019 - 30/09/2023
- URL: `https://archi-sec.telecom-paristech.fr/`
- Description: Attacks exploiting micro-architectural vulnerabilities, such as Meltdown, Spectre, Rowhammer etc, are on the rise. Modern day SoCs see an increase in complex design features, such as Branch Prediction, Out-of-Order execution, Cache coherency protocols, integrated GPUs/FPGAs, new non volatile memories. The security aspect of these new architectures and technologies remain under-studied. This project aims at modeling the architectural problems with a virtual platform based on gem5. it will be used for penetration testing, evaluate the performance cost of countermeasures, anticipate new attacks and propose protections. These latter are validated on platforms based on ARM and RISC-V processors. The major impact of this project will be through the creation of a community around our virtual platform.

5.2.6 ANR JCJC CryptAudit

- Funding: ANR
- Hosting Institution: UR1
- Budget: 222 480 EUR

- PI: Patrick Derbez
- EMSEC: Patrick, Pierre-Alain
- Period: 01/11/2017 - 31/10/2021
- URL: `https://anr.fr/Project-ANR-17-CE39-0003`
- Description: Symmetric cryptosystems are widely used because they are the only ones that can achieve some major functionalities such as high-speed or low-cost encryption, fast message authentication, and efficient hashing. But, unlike public-key cryptographic algorithms, secret-key primitives do not have satisfying security proofs. The security of those algorithms is thus empirically established by the non-discovery of attacks or weaknesses by researchers. It is obvious that this security criterion, despite its so far success, is not satisfactory, at least morally. For instance we may estimate that, for a given primitive, no more than a few dozens of researchers are actively working on breaking it. Hence, due to this weak effort, the non-discovery of an attack against a particular primitive does not mean so much. We may hope that a large class of attacks, and in particular the simplest, could be automatically discovered. The statement "we did not find any attacks of this kind" only offering a subjective guarantee could become "the audit tool X did not find any attack" which is a formal statement, giving a quantifiable objective guarantee.

  The ANR JCJC CryptAudit project is a proposal to address this concern and we aim to both develop new cryptanalytical techniques and provide a new set of open-source tools dedicated to symmetric primitives audit. More precisely we want to achieve leading researches on mainly 4 subjects: (1) Extended Demirci-Selçuk Attacks on Block Ciphers; (2) Cryptanalysis of Stream Ciphers; (3) Cryptanalysis of SHA-3; (4) Computer-aided Conception of Symmetric Primitives.

5.2.7 ANR JCJC MIAOUS

- Funding: ANR
- Hosting Institution: CNRS
- Budget: 252 860 EUR
- PI: Clémentine Maurice
- EMSEC: Clémentine, Pierre-Alain
- Period: 01/10/2019 - 31/03/2024
- URL: `https://miaous.cmaurice.fr/`
- Description: Hardware is often considered as an abstract layer that behaves correctly, executing instructions and giving an output. However, side effects due to software implementation and its execution on actual hardware can cause information leakage from side channels, resulting in critical vulnerabilities impacting both the security and privacy of these systems.

The MIAOUS project targets in particular information leakage that does not require any physical proximity to devices and that is due to processor microarchitecture, as well as the constructions of novel countermeasures. The main goal of this project is to propose a generic framework to provide a better understanding of the attack surface for microarchitectural attacks, both on the hardware and on the software side, and the tools to close the attack surface.

5.2.8 CNRS: FCS (PICS)

- Title: *Foundation of cybersecurity scripts*
- Funding: CNRS
- Hosting Institution: CNRS
- Budget: 4 000 EUR / an
- PI: Barbara Fila
- Period: 2018 – 2020
- Description: Cybersecurity is an important but also unpopular aspect of our online experience. Guidance provided to users tends to be complicated or even contradictory. The effect is that people become weary of cybersecurity and give up trying. Introduced in the 70s, scripts are what telemarketers and scammers have been using successfully in order to achieve their goals. In this project we aim at extending scripts to cybersecurity, with the goal of providing simple and efficient cybersecurity guidance to users. The objective is to define attack scripts and the corresponding counter-scripts that people can follow to stay secure in cyberspace. We will develop a formal language for scripts. It will allow us to unambiguously reason about adversarial and defensive actions, and it will be the basis to generate the guidelines for end users. In order to select the best possible counter-scripts for a given attack script, we will employ quantitative analysis techniques for security, based on attack-defense trees. "Foundations of Cybersecurity Scripts" is a three-year project funded by the CNRS PICS program, involving the EMSEC group from IRISA, the Computing, School of Science and Engineering from the University of Dundee and the Heriot-Watt University in Edinburgh, in Scotland.

5.2.9 DGA: DiscoMANIA

- Funding: DGA-MI
- Hosting Institution: CNRS
- Budget: 158 000 EUR
- PI: Clémentine Maurice
- EMSEC: Clémentine

- Period: 2018 - 2021
- Description: Microarchitectural components, such as the CPU cache, are a source of side channels on complex processors. These side channels do not require any physical access to be exploited, thus representing an important threat to modern information systems. These attacks exploit specific implementations that are leaking secret information (e.g. secret keys) by leveraging microarchitectural components. Vulnerabilities can therefore be found and patched in the software implementations, yet, as of today, the large majority of these vulnerabilities are found and subsequently fixed manually, and proposed automated methods do not scale to large software. This project aims at automating and scaling the discovery of vulnerabilities to secure software such as cryptographic libraries against microarchitectural side-channel attacks.

5.2.10 BPI: RISQ

- Funding: BPI
- Hosting Institution: UR1
- Budget: 270 000 EUR
- PI: Philippe Nguyen (Secure-IC)
- EMSEC: Pierre-Alain Fouque, Adeline Roux-Langlois, Paul Kirchner, Adela Georgescu
- Period: 01/01/2017 - 30/09/2020
- URL: `https://risq.fr/?page_id=31&lang=en`
- Description: Cryptography is the cornerstone for securing data and digital exchanges. The coming of a quantum computer, that relies on different physical concepts, threatens most of those applications. Henceforth, substantial technical developments change must occur over the following years. These changes must guarantee to those fields an acceptable and lasting level of security and ensure digital exchange confidentiality and user privacy. The RISQ project applies to every field of technology employing cryptographic methods. The outcome of this project will include an exhaustive encryption and transaction signature product line, as well as an adaptation of the TLS protocol. Hardware and software cryptographic solutions meeting these constraints in terms of security and embedded integration will also be included. Furthermore, documents guiding industrials on the integration of these post-quantum technologies into complex systems (defense, cloud, identity and payment markets) will be produced, as well as reports on the activities of standardization committees.

5.2.11 CominLabs : TYREX

- Funding: CominLabs

- Hosting Institution: CNRS
- Budget: 88 000 EUR
- PI: Adeline Roux-Langlois
- EMSEC: Adeline
- Period: 01/05/2017 - 30/11/2019
- Description: Post-quantum security has been pointed out as a crucial issue by the NIST. Several tracks have been derived to address this issue, among which Euclidean lattices is particularly promising. Moreover, this mathematical structure provides efficient encryption schemes which enable to process data in a non trivial way while it is encrypted. These schemes are called Fully Homomorphic Encryption (FHE) schemes, and in practice, several issues have still to be addressed to propose practical solutions, but things evolve quickly. Hence, anyone that would like to use this technology will be interested by new results on the security analysis of these schemes. To reach these results, the core of this collaboration will be to study in details the hardness of lattice problems in ideal lattices.

5.2.12 CPER

- Funding: UE, Région, Département, Rennes Métropole.
- PI EMSEC: Pierre-Alain Fouque and Gildas Avoine
- Hosting Institution: 65 000 EUR UR1 and 200 000 EUR INSA Rennes
- Period: 2015 - 2020
- Description: The CPER SSI (Contrat de plan Etat-région Sécurité des Systèmes d'Information) is a Brittany-focused project that aims to consolidate and develop research activities in cybersecurity in Brittany. The CPER so aims to develop and provide access to new technology platforms and tools for cybersecurity research and training, and consolidate and develop synergies between Brittany's laboratories through the development of shared platforms.

5.3 Bilateral industry grants

- Grant Orange Labs, Loïc Ferreira
  The objective of this collaborative work is to analyze and design lightweight cryptographic primitives and protocols for the Internet of Things. In particular, we aim to design a protocol to allow two connected parties to establish secure channels, typically between a server and a smartcard. Such a channel should take the capacities into account, in terms of computation, communication, and storage.
- Grant CIFRE Orange Labs, Olivier Gimenez
  The objective of this collaborative work is to design solutions to detect traffic diversion in 5G networks. The expected solution is based on the round-trip time

of cryptographic messages exchanged over the network. Abnormal behaviors can so be detected using a statistical approach.

- Grant CIFRE Orange Labs, Guillaume Kaim
  The objective of this collaboration is to work on post-quantum private-life protection, in particular on the topics of the PROMETHEUS H2020 project. The main goal is to build cryptographic constructions which are secure and efficient in this context. In particular, Guillaume worked on lattice-based blind signature, their applications to e-voting and on group signatures.

- Grant CIFRE Orange Labs, Adina Nedelcu
  The objective of this collaboration is to study the TLS protocol in the SafeTLS project by studying the anonymity achieved by the new version TLS 1.3 and to look at the lawful interception problem. The main problem is that TLS is an end-to-end encryption protocol which means that the middle box security products such as malware analysis cannot be used to perform traffic analysis. The lawful interception problem is crucial for the security of 5G network as the protocol has to provide proof that the network operator is able to remove the encryption layer.

- Grant CIFRE Amossys, Alban Siffer
  The objective of this collaboration work is to study data mining techniques in order to detect Advanced Persistent Threat (APT), which are very efficient attacks that are not detected using signature based approach since they are not known today. For that, we use extreme value theory to detect a drift in the distribution function independently of the original function and detect rare events.

5.4 Collaborations

5.4.1 Visited Labs

- Pierre-Alain Fouque visited NTT (Japan) during 2 days in April 2019.
- Barbara Fila visited the University of Dundee (Scotland) on 19–22 August 2019.
- Katharina Boudgoust visited the Monash University (Australia) on October-December 2019 (3 months)
- Olivier Bernard visited ENS Lyon during one month in October 2019.
- Alexandre Debant visited the University of Birmingham (UK) on August-September 2019 (5 weeks)
- Stéphanie Delaune visited the University of Surrey (UK) on 28-31 October 2019.
- Patrick Derbez visited NTT (Japan) during on 16–20 December 2019.

5.4.2 Visiting researchers

- Sasa Radomirovic from the University of Dundee (Scotland) visited Barbara Fila on 2–8 June and 16–21 July 2019.

- Ioana Boureanu from the University of Surrey (UK) visited Stéphanie Delaune on 9-12 July 2019.
- Mehdi Tibouchi from NTT (Japan) visited Pierre-Alain Fouque on 18-20 November 2019.
- Tom Chothia from the University of Birmingham (UK) visited Stéphanie Delaune on 9-12 July 2019.

6 Dissemination

6.1 Promoting scientific activities

- Gildas Avoine is a member of the *Institut Universitaire de France*. He is also the director of the CNRS' GDR (national scientific network) in computer security (1300+ researchers), and the president of the scientific council of the French agency ANSSI devoted to cybersecurity. He belongs to the cybersecurity workgroup of Allistene (*Alliance des sciences et technologies du numérique*). He was also elected to both research and teaching councils in computer science at INSA Rennes.
- Pierre-Alain Fouque is a member of the *Institut Universitaire de France*. He is also Responsible for the Master Cybersécurité at Rennes 1 University and for the new international Master in Cybersecurity within the EIT Digital umbrella. He was the PI for the ANR SafeTLS projects and works in the Prometheus European Project. He was the co-Program Chair of CHES 2019 with 4 submission deadlines during the 2018-19 academic year and is a member of the steering committee board of CHES. He was a member of the evaluation committee for the European Research Council. He was a member of the MathCrypt and ToSC program committees. He presented the EUR CyberSchool project (École Universitaire de Recherche) which has been accepted by ANR in August 2019 for 5,750,000 euros in order to consolidate the teaching in cybersecurity in the Rennes area.
- Stéphanie Delaune is the PI of the ERC POPSTAR (2017-2022), and the local PI of the ANR TECAP (2018-2022). She was a member of SEC@SAC, and ESORICS program committees. She was also the program chair of CSF (with Limin Jia). Since 2016, she is a member of the IFIP WG-1.7 Foundations of Security Analysis, and she joined the steering committee of CSF in 2017. In 2018, she joined the steering committee of POST and PLAS, and the editorial board of the journal ACM TOCL, as well as IPL. In 2019, she receives the outstanding community service award from the IEEE technical committee on Security and Privacy. At the national level, she is member of the executive board of the GDR Sécurité Informatique and in particular she in charge of the working group "Méthodes Formelles pour la Sécurité". She is also a member of the scientific council of the GDR-IM. At the local level, she is now head of the CyberSecurity axis, and an elected member of the laboratory council.
- Clémentine Maurice is the PI of the JCJC ANR project MIAOUS as well as the local PI of the ANR project ARCHI-SEC. She is the co-chair of the PhD Award

"Gilles Kahn" of the *Société Informatique de France*. She organized the Summer Shool on the Security of Hardware/Software Interface (SILM). She was co-chair of WOOT'19 where she organized the first Artifact Evaluation, and co-chair of DIMVA'19. She was involved in the program committees of SSTIC'19, EuroSec'19 and S&P'20. She was an invited lecturer at the Ben-Gurion University (Israel), and gave invited presentations at INSA Toulouse, and at the FICHSA Conference (Israel).

- Patrick Derbez is the PI of the JCJC ANR project CryptAudit as well as the local PI of the ANR project Decrypt. He is a PC member of ToSC IACR journal.

- Barbara Fila gave an invited tutorial at the *16th International Conference on Quantitative Evaluation of Systems* (QEST'19), on September 11, 2019, in Glasgow, UK. In March 20419, she was also an invited lecturer at the *24th Estonian Winter School in Computer Science* (EWSCS'19), Palmse, Estonia. In 2019, she was member of the program committee of DBSec'19 and GraMSec'19. She reviewed for CSF'20, FASE'20, GraMSec'19, SEC@SAC'20, TrustCom'19, DBSec'19. Barbara was a member of the the selection committee for an assistant professor (MCF) position at ENSIBS Vannes. Since 2016, Barbara is a co-chair of the *Software and Systems Security* (SoSySec) seminar (https://seminaires-dga.inria.fr/en/sosysec-en-bref/) organized as part of the general partnership agreement between the *Cyber Pole of Excellence* (PEC), Inria, and DGA-MI.

- Adeline Roux-Langlois is co-responsible of the Cryptography Seminar (DGA, IRMAR, IRISA) in Rennes. She was also member of the scientific committee of the CCA seminar (organised by the GT-C2) which is in Paris (4 times a year), and of the organisation committee of the WCC international workshop (St Jacut de la mer, April 2019). She was a PC member of the CRYPTO, Africacrypt and IMACC conferences. She was invited speaker at the "Journées nationales du GDR Sécurité" in Paris.

6.2 Teaching and Juries

6.2.1 Teaching

- Gildas Avoine is in charge of the 10-hour course "Network Security" (4th-year students) and the 26-hour course "Cryptographic Engineering" (4th-year students) both at INSA Rennes. He also taught "Security" in 2019 at NYU Paris.
- Stéphanie Delaune co-lectures (with Barbara Fila) the 26-hour course "Verification of security protocols" (5th-year students, INSA Rennes), and the 20-hour course "Security protocols" (5th-year students, Master SIF, University Rennes 1). She also gives 32h to supervise a project at INSA on security protocols verification (4-th year students).
- Patrick Derbez is in charge of a 48-hour course "Algorithms for Security" (4th-year students) and of a 12-hour course "Symmetric cryptography" (5th-year students), both at the University of Rennes.

- Pierre-Alain Fouque is in charge of a 32-hour course "Introduction to Cryptography" (5th-year students) and in charge of a 48-hour course "Introduction to Security" (4th-year students) at Rennes University. He is involved in a Mathematical Computation course at ENS Rennes for 20 hours and is co-responsible for the course of imperative programming in Java for all first-year students in the Maths and CS departments of the Rennes 1 University with Patrick Derbez.
- Barbara Fila co-lectures and is in charge of the 32-hour course "Languages and grammars" (4th-year students, INSA Rennes), the 26-hour course "Verification of security protocols" (5th-year students, INSA Rennes), and the 20-hour course "Security protocols" (5th-year students, Master SIF, University Rennes 1). She also is the administrative coordinator of the "Secure programing" course (4th-year students, INSA Rennes).
- Clémentine Maurice is in charge of a 16-hour course on "Security" (L3 students, ENS Rennes), and gives 10 hours of lectures and 6 hours of labs in the course "Side-Channel Attacks" (5th year students, INSA Rennes).
- Adeline Roux-Langlois is in charge of a 24-hour course on "Introduction to Cryptography" (1st year students at ENS Rennes) and co-lecture 24 hours in a 32h course "Lattices for cryptography" (5th year students, UR1).
- Mohamed Sabt is in charge of three 48-hour courses for 4th-year students at the University of Rennes 1 within the international Master Cybersecurity of EIT Digital: "Networks Security", "Software Security" and "System Security".

6.2.2 PhD and HDR Juries

- Kevin Bukasa, UR1, May 2019 (Pierre-Alain Fouque was "President")
- Lukasz Michal Chmielewski, Ninegen (Netherlands), August 2019 (Pierre-Alain Fouque was "Reviewer")
- Romain Gay, ENS, March 2019 (Pierre-Alain Fouque was "President")
- Nisrine Jafri, UR1, March 2019 (Pierre-Alain Fouque was "President")
- Louiza Khati, ENS, July 2019 (Pierre-Alain Fouque was "Reviewer")
- Fabio Pagani, EURECOM, September 2019 (Clémentine Maurice was "Examinatrice")
- Razvan Rosie, ENS, May 2019 (Pierre-Alain Fouque was "President")
- Florent Tardif, UR1, November 2019 (Pierre-Alain Fouque was "President")
- Jorge Toro-Pozo, Luxembourg University, May 2019 (Stéphanie Delaune was "Reviewer").
- Mathieu Valois, Normandie Université, December 2019 (Gildas Avoine was "Examinateur")
- Antoine Vastel, Université de Lille, October 2019 (Clémentine Maurice was "Examinatrice")

6.3 Popularization

- Gildas Avoine is the co-author with Cédric Lauradoux and Rolando Trujillo-Rasua of the article "Should Chess Players Learn Computer Security?" published in Hakin9, Vol 13, No 10, 2019.
- Gildas Avoine participated to a panel about smart cities in the framework of the European Cyber Week, Rennes, November 2019.
- Gildas Avoine gave a half-day training about computer security to the financial service of Inria RBA, Carnac, May 2019.
- Gildas Avoine was invited to "petit-déjeuner parlementaire" to answer questions from members of the parliament belonging to the "office parlementaire d'évaluation des choix scientifiques et technologiques".
- Stéphanie Delaune gave a talk to a group of 15 students to explain her research (accueil réalisé à l'IRISA dans le cadre du stage de 3ème).

6.4 Responsible Disclosure

- Mohamed Sabt and Pierre-Alain Fouque informed GlobalPlatform about the different vulnerabilities identified in their standard. Several companies, especially in Japan, deploy the protocol that we studied. Therefore, we collaborated with GlobalPlatform and NTT Data in order to write a new version of the protocol that mitigates our vulnerabilities. We are proofreading the latest version that will be published soon.
- Mohamed Sabt informed the different service providers that implement the Remember Me feature of FIDO U2F. The service providers have ignored our warnings. However, following our presentation in SSTIC 2020, the FIDO Alliance started a new collaboration with us in order to include a secure version of the Remember Me feature into the certification process. Such a new standard will force all the complying service providers to implement our proposed solution.
- Mohamed Sabt and Pierre-Alain Fouque informed Intel about some identified vulnerabilities within their implementation of Linux Wifi daemon. Indeed, the implementation that is already integrated into Arch Linux for instance is vulnerable to cache attacks. The discussion is still in progress to mitigate our findings.

7 Bibliography

Books and Monographs

[1] G. Cybenko, D. J. Pim, B. Fila (editors), *5th International Workshop on Graphical Models for Security (GraMSec) 2018, held in conjunction with the Federated Logic Conference (FLoC) 2018, Oxford, UK, July 8, 2018, Revised Selected Papers*, April 2019, `https://hal.inria.fr/hal-02115721`.

[2] A. Gantman, C. Maurice (editors), *13th USENIX Workshop on Offensive Technologies, WOOT 2019, Santa Clara, CA, USA, August 12-13, 2019*, USENIX Association, 2019, https://www.usenix.org/conference/woot19.

[3] R. Perdisci, C. Maurice, G. Giacinto, M. Almgren (editors), *Detection of Intrusions and Malware, and Vulnerability Assessment - 16th International Conference, DIMVA 2019, Gothenburg, Sweden, June 19-20, 2019, Proceedings*, *Lecture Notes in Computer Science*, *11543*, Springer, 2019, https://doi.org/10.1007/978-3-030-22038-9.

Doctoral dissertations and "Habilitation" theses

[4] P. Bert, *Signature reposant sur les réseaux euclidiens : de la construction à l'implémentation*, PhD Thesis, November 2019.

[5] L. Ferreira, *Secure Tunnels for Constrained Environments*, PhD Thesis, November 2019.

[6] B. Lambin, *Optimization of core components of block ciphers*, PhD Thesis, October 2019.

[7] C. Qian, *Lossy trapdoor primitives, zero-knowledge proofs and applications.*, PhD Thesis, October 2019.

[8] A. Siffer, *New statistical methods for data mining, contribution to anomaly detection and unimodality testing*, PhD Thesis, December 2019.

[9] F. Tardif, *Practical Considerations on Cryptanalytic Time-Memory Trade-Offs*, PhD Thesis, November 2019.

[10] W. Widel, *Formal modeling and quantitative analysis of security using attack–defense trees*, PhD Thesis, December 2019.

Articles in referred journals and book chapters

[11] G. Arfaoui, X. Bultel, P.-A. Fouque, A. Nedelcu, C. Onete, "The privacy of the TLS 1.3 protocol", *Proceedings on Privacy Enhancing Technologies 2019*, 2019, p. 190 – 210, https://hal.archives-ouvertes.fr/hal-02482253.

[12] G. Avoine, J. Munilla, A. Peinado, K. B. Rasmussen, D. Singelee, A. Tchamkerten, R. Trujillo-Rasua, S. Vaudenay, M. A. Bingöl, I. Boureanu, S. čapkun, G. Hancke, S. Kardaş, C. H. Kim, C. Lauradoux, B. Martin, "Security of Distance-Bounding: A Survey", *ACM Computing Surveys 51*, 5, January 2019, p. 1–33, https://hal.archives-ouvertes.fr/hal-02470057.

[13] R. Bost, P. Fouque, "Security-Efficiency Tradeoffs in Searchable Encryption", *PoPETs 2019*, 4, 2019, p. 132–151, https://doi.org/10.2478/popets-2019-0062.

[14] R. Chrétien, V. Cortier, A. Dallon, S. Delaune, "Typing messages for free in security protocols", *ACM Transactions on Computational Logic 21*, 1, 2019, https://hal.inria.fr/hal-02268400.

[15] P.-A. Fouque, M. Tibouchi, "Close to Uniform Prime Number Generation With Fewer Random Bits.", *IEEE Transactions on Information Theory 65*, 2, December 2019, p. 1307–1317, https://hal.inria.fr/hal-02470839.

[16] L. Hirschi, D. Baelde, S. Delaune, "A method for unbounded verification of privacy-type properties", *Journal of Computer Security 27*, 3, June 2019, p. 277–342, https://hal.inria.fr/hal-02368832.

[17] P. Laperdrix, G. Avoine, B. Baudry, N. Nikiforakis, "Morellian Analysis for Browsers: Making Web Authentication Stronger with Canvas Fingerprinting", *in : Detection of Intrusions and Malware, and Vulnerability Assessment - 16th International Conference, DIMVA 2019, Gothenburg, Sweden, June 19-20, 2019, Proceedings*, June 2019, p. 43–66, https://hal.archives-ouvertes.fr/hal-02881632.

[18] W. Widel, M. Audinot, B. Fila, S. Pinchinat, "Beyond 2014: Formal Methods for Attack Tree-based Security Modeling", *ACM Computing Surveys 52*, 4, September 2019, p. 1–36, https://hal.archives-ouvertes.fr/hal-02308427.

Publications in Conferences and Workshops

[19] G. Avoine, S. Canard, L. Ferreira, "IoT-Friendly AKE: Forward Secrecy and Session Resumption Meet Symmetric-Key Cryptography", *in : Computer Security – ESORICS 2019*, p. 463–483, Luxembourg, Luxembourg, September 2019, https://hal.archives-ouvertes.fr/hal-02470056.

[20] S. Bai, K. Boudgoust, D. Das, A. Roux-Langlois, W. Wen, Z. Zhang, "Middle-Product Learning with Rounding Problem and Its Applications", *in : Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part I*, S. D. Galbraith, S. Moriai (editors), *Lecture Notes in Computer Science, 11921*, Springer, p. 55–81, 2019, https://doi.org/10.1007/978-3-030-34578-5_3.

[21] S. Bai, S. Miller, W. Wen, "A Refined Analysis of the Cost for Solving LWE via uSVP", *in : Progress in Cryptology - AFRICACRYPT 2019 - 11th International Conference on Cryptology in Africa, Rabat, Morocco, July 9-11, 2019, Proceedings*, J. Buchmann, A. Nitaj, T. Rachidi (editors), *Lecture Notes in Computer Science, 11627*, Springer, p. 181–205, 2019, https://doi.org/10.1007/978-3-030-23696-0_10.

[22] G. Barthe, S. Belaïd, G. Cassiers, P.-A. Fouque, B. Grégoire, F.-X. Standaert, "Automated Verification of Higher-Order Masking in Presence of Physical Defaults", *in : ESORICS 2019 - 24th European Symposium on Research in Computer Security*, p. 300–318, Luxembourg, Luxembourg, September 2019, https://hal.archives-ouvertes.fr/hal-02404662.

[23] G. Barthe, S. Belaïd, T. Espitau, P.-A. Fouque, M. Rossi, M. Tibouchi, "GALACTICS: Gaussian Sampling for Lattice-Based Constant- Time Implementation of Cryptographic Signatures, Revisited.", *in : CCS 2019*, p. 2147–2164, Copenhague, Denmark, May 2019, https://hal.inria.fr/hal-02470947.

[24] O. Blazy, A. Bossuat, X. Bultel, P.-A. Fouque, C. Onete, E. Pagnin, "SAID: Reshaping Signal into an Identity-Based Asynchronous Messaging Protocol with Authenticated Ratcheting", *in : IEEE European Symposium on Security and Privacy, EuroS&P 2019, Stockholm, Sweden, June 17-19, 2019*, IEEE, p. 294–309, Stockholm, Sweden, 2019, https://hal.archives-ouvertes.fr/hal-02307142.

[25] X. Bultel, P. Lafourcade, R. W. F. Lai, G. Malavolta, D. Schröder, S. Aravinda, K. Thyagarajan, "Efficient Invisible and Unlinkable Sanitizable Signatures", *in : International Conference on Practice and Theory in Public Key Cryptography PKC'19*, Beijin, China, 2019, https://hal.archives-ouvertes.fr/hal-01964514.

[26] A. Debant, S. Delaune, C. Wiedling, "Symbolic analysis of terrorist fraud resistance", *in : Computer Security - ESORICS 2019 - 24th European Symposium on Research in Computer Security*, Luxembourg, Luxembourg, September 2019, https://hal.inria.fr/hal-02171218.

[27] A. Debant, S. Delaune, "Symbolic verification of distance bounding protocols", *in : Principles of Security and Trust - 8th International Conference, 11426*, Prague, Czech Republic, April 2019, https://hal.inria.fr/hal-02018280.

[28] P. Derbez, P.-A. Fouque, B. Lambin, V. Mollimard, "Efficient Search for Optimal Diffusion Layers of Generalized Feistel Networks", *in : IACR Transactions on Symmetric Cryptology*, Athènes, Greece, 2019, https://hal.archives-ouvertes.fr/hal-02162306.

[29] P. Derbez, V. Lallemand, A. Udovenko, "Cryptanalysis of SKINNY in the Framework of the SKINNY 2018-2019 Cryptanalysis Competition", *in : SAC 2019 - Selected Areas in Cryptography*, Waterloo, Canada, August 2019, https://hal.inria.fr/hal-02388239.

[30] B. Fila, W. Widel, "Attack–defense trees for abusing optical power meters: A case study and the OSEAD tool experience report", *in : Graphical Models for Security*, Hoboken, United States, June 2019, https://hal.inria.fr/hal-02872275.

[31] B. Fila, W. Widel, "Efficient Attack–Defense Tree Analysis using Pareto Attribute Domains", *in : 2019 IEEE 32nd Computer Security Foundations Symposium (CSF)*, IEEE, p. 200–215, Hoboken, United States, June 2019, https://hal.archives-ouvertes.fr/hal-02308407.

[32] C. Genevey-Metat, B. Gérard, A. Heuser, "Combining sources of side-channel information", *in : C&ESAR 2019*, Rennes, France, November 2019, https://hal.archives-ouvertes.fr/hal-02456646.

[33] B. Libert, C. Qian, "Lossy Algebraic Filters With Short Tags", *in : PKC 2019 - 22nd International Conference on Practice and Theory of Public Key Cryptography, LNCS, 11442*, Springer, p. 34–65, Beijing, China, April 2019, https://hal.inria.fr/hal-02124968.

[34] V. Migliore, B. Gérard, M. Tibouchi, P. Fouque, "Masking Dilithium - Efficient Implementation and Side-Channel Evaluation", *in : Applied Cryptography and Network Security - 17th International Conference, ACNS 2019, Bogota, Colombia, June 5-7, 2019, Proceedings*, R. H. Deng, V. Gauthier-Umaña, M. Ochoa, M. Yung (editors), *Lecture Notes in Computer Science, 11464*, Springer, p. 344–362, 2019, https://doi.org/10.1007/978-3-030-21568-2_17.

[35] S. Pinchinat, B. Fila, f. F. Wacheux, Y. Thierry-Mieg, "Attack Trees: A Notion of Missing Attacks", *in : GraMSec 2019 - 6th International Workshop on Graphical Models for Security, Lecture Notes in Computer Science, 11720*, p. 23–49, Hoboken, NJ, United States, June 2019, https://hal.archives-ouvertes.fr/hal-02533750.

Miscellaneous

[36] G. Avoine, C. Lauradoux, T.-R. Rolando, "Should Chess Players Learn Computer Security?", February 2019, Hacking it security magazine, https://hal.inria.fr/hal-02082837.

[37] T. Richmond, A. Heuser, B. Gérard, "Side-Channel Analysis of Post-Quantum Cryptography", SecDays 2019 – Security Days, January 2019, Poster, https://hal.inria.fr/hal-02018859.