Activity Report 2017

Team EMSEC

Embedded Security & Cryptography

D1 – Large Scale Systems

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 Kordy (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

EMSEC's co-leaders are Gildas Avoine and Pierre-Alain Fouque.

Associate members

Benoît Gérard	Jan 2016 to Sep 2020	DGA-MI

PhD students

Pauline Bert	Sep 2016 to Sep 2019	Bourse DGA
Angèle Bossuat	Sep 2017 to Sep 2020	Bourse DGA
Raphaël Bost	Sep 2014 to Jan 2018	DGA
Qian Chen	Sep 2016 to Sep 2019	Bourse ENS
Alexandre Debant	Oct 2017 to Sep 2020	ERC POPSTAR
Claire Delaplace	Sep 2014 to Sep 2017	ANR Brutus
Loïc Ferreira	Oct 2016 to Sep 2019	Orange Labs
Thomas Gougeon	Sep 2014 to Aug 2017	MENRT
Guillaume Kaim	Oct 2017 to Sep 2020	Orange Labs
Baptiste Lambin	Sep 2016 to Sep 2019	Bourse DGA
Benjamin Richard	Dec 2013 to Feb 2017	Orange Labs
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

Vincent Migliore	Oct 2017 to Aug 2018	BPI RISQ
Cristina Onete	Sep 2015 to Aug 2017	Bourse Région + ANR SafeTLS
Mohamed Sabt	Oct 2017 to Aug 2018	CominLabs TYREX
Cyrille Wiedling	Jan 2016 to Aug 2017	DGA grant + ERC POPSTAR

Administrative assistant

Cécile Bouton

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.

Topics of cybersecurity are extremely varied. Several classifications exist because they can be based on the underlying domains (computer science, mathematics, electronics, etc.), on the scientific tools (formal methods, cryptography, etc.), on the objectives to be achieved (protection of privacy, authentication, watermarking, etc.), or on the application fields (control of industrial processes, access control, etc.). For example, *security and privacy* is one of twelve major IT themes that appears in the 2012 ACM Computing Classification System. It is then divided into (1) Cryptography, (2) Formal methods and theory of security, (3) Security services, (4) Intrusion/anomaly detection and malware mitigation, (5) Security in hardware, (6) Systems security, (7) Network security, (8) Database and storage security, (9) Software and application security, (10) Human and social aspects of security and privacy.

EMSEC's core activities focus on (1) Cryptography, (2) Formal methods and theory of security, (5) Security in hardware, and (6) Systems security. Other topics are considered, though, through collaborations. Our research activities are more specifically organized along three axes: **Cryptography**, **Formal Methods**, and **Security of Hardware and Software Systems**. This report details these three axes in what follows. This wide competence spectrum allows EMSEC to address security issues from an holistic approach, from theory to practice.

2.2 Scientific foundations

We develop in the EMSEC three complementary research directions. The first axis concern fundamental results in symmetric and asymmetric cryptology.

2.2.1 Cryptology

In Cryptography, the EMSEC team is strongly involved in the two important NIST competitions concerning the security of post-quantum schemes and of lightweight ciphers. In particular, we proposed the Falcon signature scheme based on structured lattices. We are very active in the European Prometheus and BPI RISQ projects in order to construct new schemes with anonymity properties based on lattices or to evaluate the security of these schemes by studying the algorithms to solve them and by looking carefully on the implementation of these cryptographic schemes. Within the ANR JCJC CryptAudit and the new ANR Decrypt project, we study the resistance of lightweight symmetric ciphers using automatic tools, including MILP or CSP solvers.

Asymmetric primitives. Thanks to all the projects on lattice cryptography (TYREX, RISQ and Prometheus) we had fundings to hire many PhD and postdoc candidates. We work essentially on two different directions.

On the first direction, we designed 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. NIST is also considering a new call for Threshold Cryptography and it would be nice to study if we can do it with lattice assumptions and with Falcon for instance.

We have also worked on the security of cryptographic implementation of lattice schemes. We studied the core component of efficient lattice schemes such as Gaussian sampling against timing attack. We look at 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.

Symmetric primitives. Within the ANR CryptAudit and Decrypt, we study the security of symmetric ciphers. We have looked at the key schedule part of the AES block cipher and we proposed more efficient constructions against classical attacks. Then, we have also studied the more powerful white-box model and we proposed some attacks on one recent proposal as well as a generic attack. Finally, we have also considered and refined division property based attacks on block ciphers such as PRESENT, GIFT, RECTANGLE and MiDORI.

Protocols. We worked on two subjects within the SafeTLS project: the first one concerns the security of TLS and the second one the security of new messaging protocol. On the security of cryptographic protocols, we get new results about the recent TLS 1.3 standard with respect to middleboxes and we study WhatsApp security.

Reduction and Assumptions. We are interested in studying the security of the assumptions used in lattices or the hard problems. On the first direction, we prove some reductions between hard problems and we also try to solve these hard problems.

2.2.2 Formal Methods & 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.

Verification of cryptographic protocols. One extremely successful approach when designing and analysing security protocols, is the use of formal methods. The purpose of formal verification is to provide rigorous frameworks and techniques to analyse 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 characterise 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 modelled and analysed. 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 analyse modern protocols. For instance, many modern protocols rely on a notion of state or time, and can not be analysed using existing verification tools. Moreover, techniques to analyse privacy-type properties which are expressed relying on behavioural 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 [KPCS14] 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.

[KPCS14] B. Kordy, L. Piètre-Cambacédès, P. Schweitzer, "DAG-Based Attack and Defense Modeling: Don't Miss the Forest for the Attack Trees", *Computer Science Review 13–14*, 0, 2014, p. 1–38.

2.2.3 Software / Hardware System Security

Security of cryptographic implementations. Cryptographers are able to design schemes and protocols that are secure – although working on new research directions as post-quantum or more efficient schemes is still of the utmost importance. However the security of the implementations is a much more 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 SCA protection, it is possible to break it in practical time. In the traditional cryptographic scenario, the attacker has black-box access to the device storing the secret key and tries to recover the key given inputs/outputs of a function parametrized by a secret key. 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. The two recently hired members, Clémentine Maurice (2017) and Mohamed Sabt (2018), bring new important contributions on this domain.

Attack techniques. 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.

The second generic attack EMSEC considers is the **cryptanalytic time-memory trade-off** (TMTO) technique. 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.

Data security & machine learning Among the odds and ends topics considered by EMSEC, there is a growing branch of activities related to data security and machine learning techniques, making EMSEC more and more competent in retrieving information in large data sets, whatever the data sets can be. For example, we work with Raphaël Bost on the security of database and we study symmetric searchable encryption schemes. With Alban Siffer, we propose new statistical tools to detect shift in a timing series or anomaly. This problem is related to supervision and we proposed several algorithms. EMSEC also has activities in the field of **data desanonymisation**, in collaboration with Tristan Allard and Elisa Fromont (IRISA). Finally, EMSEC also works on **forensics** applied to smartcards, in collaboration with the e-payment and biometrics research group (GREYC, Caen), where the objective is to retrieve information in a memory dump extracted from an EEPROM.

3 Scientific achievements

Cryptography

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. At this stage, we analyze existing solutions, and we submitted to a conference an attack against the protocol Lorawan 1.0.

3.1 Symmetric Cryptography

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

Collaborations: LORIA (Nancy), EMN (Nantes), Meiqin Wang (China), Siwei Sun (China) , Yosuke Todo (NTT Japan).

In the ANR JCJC CryptAudit and the ANR BRUTUS and ANR DECRYPT projects, the goal is to study the resistance of block ciphers. In the BRUTUS project, we propose new attacks and construction for white-box cryptography. One paper has been accepted at CHES 2018, another has been distinguished as the 3 best papers of ASIACRYPT 2015 and the journal version appears in 2018.

We also build new tools for automatically searching some attacks or distinguishers. In the new projects DECRYPT, we use MILP or Constrained Programming Tools for this task as they allow to represent constraints 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 for cryptographic problems. Patrick has already used CP tools to look for Demirci-Selçuk attacks at ASIACRYPT 2018. He has also attacked a pseudo-random function based on AES at FSE 2018.

In the CryptAudit project, we construct specific tools for the same task. One important application of these techniques is the search of division properties. We also generalize these attacks as they are not invariant by linear applications contrary to previous attacks. We also propose more efficient and secure variant for the key schedule algorithm of AES at SAC 2018 and more recently we study the diffusion property of generalized Feistel, solving a 10-year open problem in this area.

3.2 Real-World Cryptography

Participants: Pierre-Alain Fouque, Céline Duguet, Angèle Bossuat, Adina Nedelcu.

Collaborations: XLIM (Limoges), Bourges, Inria (Paris) 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.

Middleboxes are network components analyzing the data stream as malware analysis or content-delivery network. However, since TLS is an end-to-end encryption protocol, such middleboxes cannot be used anymore and if we want to use such elements securely, new protocols and security assurance need to be defined. We published one paper at EuroSP 2016 specific to Content-Delivery Network protocols such as CloudFlare and Akamai and another at S&P 2018 for more general applications. At ASIACRYPT 2018 we also proposed a less efficient solution but with pattern matching capabilities. New papers have been recently published on this problem.

We begin a new research direction on the security of Messaging protocols, such as Signal. The security of WhatsApp is today an important subject and the IETF is working on the new Message Layer Security standard. We identify some vulnerabilities and we propose to fix them using an Identity-Based signature schemes and more authentication information in the key derivation function. We also look at the security of multi-devices for Signal and we propose more efficient protocols. Finally, we study the security of the MLS protocol and we develop some proofs to avoid malicious server and minimize the trust assumptions.

3.3 Cryptanalysis of Public-Key Cryptography

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

Collaborations: Thomas Espitau, Alexandre Gélin (Sorbonne University), Damien Stehlé (ENS Lyon), Martin Albrecht (RHUL).

We study hard problems recently proposed in cryptography to build schemes with new properties. In particular, we proposed new attacks on overstretched NTRU schemes widely used for Fully Homomorphic Encryption (FHE) Schemes at EUROCRYPT 2017 and we broke numerous schemes. The idea is that in these lattices we have many short vectors. More recently, we broke many FHE schemes based on large integers.

We also consider new algorithmic problems in Number Theory such as finding the generator of a principal ideal in the integer ring of cyclotomic number fields since finding the secret-key in Smart-Vercauteren FHE scheme is based on this problem. We broke real parameters proposed for this scheme a EUROCRYPT 2017.

More recently, we propose an algorithm for reducing algebraic lattice and we show that we can take into account the special structure to design efficient algorithm in practice. We implemented this algorithm and we were able to break some scheme proposed for multi-linear applications. We also proposed another algorithm for a multi-linear schemes based on large integers at EUROCRYPT 2016.

Finally, we have also proposed an asymptotically more efficient BKZ and enumeration algorithms.

3.4 Design of Public/Symmetric Key Cryptography

Participants: Pauline Bert, Katharina Boudgoust, Claire Delaplace, Pierre-Alain Fouque, Paul Kirchner, Chen Qian, Adeline Roux-Langlois, Mohamed Sabt, Weiqiang Wen, Yang Yu.

Collaborations: Charles Bouillaguet (Lille University), Benoît Libert (ENS Lyon).

We propose at PQCrypto 2018 a new signature scheme based on the Ring-LWE problem with Pauline, Adeline and Mohamed. This scheme is not as efficient as the Falcon scheme, also based on the GPV framework, but it seems to be more secure since it is based on a stronger assumption.

With Claire Delaplace, Charles Bouillaguet and Paul Kirchner, we also propose an efficient symmetric scheme at PQCrypto 2017 for based on a lattice-based public-key assumption which is called LWR (Learning with Rounding). It is as efficient as AES on computers where there is no AES instructions.

With Paul Kirchner and many people, we propose the Falcon signature scheme at the NIST Post-Quantum Competititon in October 2017. This scheme is still selected for the second round of the competition. More recently, we extend this scheme to a compact variant of the NTRU encryption scheme with Yang Yu and we propose a more compact signature scheme.

Chen and Benoît Libert have proposed many security proofs on public-key cryptographic constructions such as structure-preserving chosen ciphertext security with shorter verifiable ciphertext at PKC 2017 and ring signature of logarithmic size with tight security at ESORICS 2018.

3.5 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 SCO02[AF18a]. The design of a new protocol with the matching security model is in progress.

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

3.6 Distance Bounding Protocol Design

Participants: Gildas Avoine, Cristina Onete.

Collaborations: TÜBİTAK BİLGEM (Turkey), University of Luxembourg, UQAM (Canada), ETS Montréal (Canada), Université Clermont Auvergne (France).

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* (See Figure 1). 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 designs distance bounding protocols that either benefit from a proof or improve existing ones in terms of performance[ABG+17,ABK+11,].

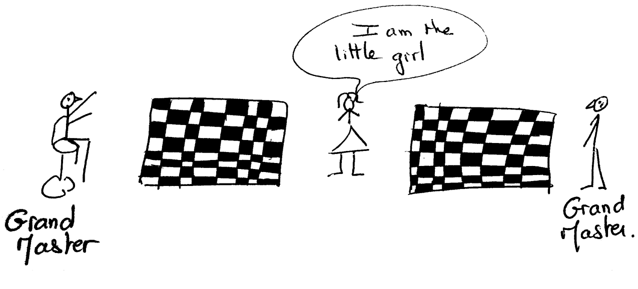


Figure 1: Chess Grand Master Problem

[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.

3.7 Symbolic analysis of distance bounding protocols

Participants: Alexandre Debant, Stéphanie Delaune, Cyrille Wiedling.

Collaborations: Cyrille Wiedling.

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 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. These reduction results allow one to use verification tools (e.g. ProVerif, Tamarin) developed for analysing more classical security properties [DDW18]. 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. As an application, we analyse several distance bounding protocols, as well as some contactless payment protocols.

3.8 Deciding equivalence-based properties in the bounded setting

Participants: Stéphanie Delaune.

Collaborations: David Baelde (MdC, ENS Paris Saclay), Véronique Cortier (DR CNRS, LORIA), Steve Kremer (DR Inria, LORIA) Antoine Dallon, Ivan Gazeau, Lucca Hirshi.

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.

[DDW18] A. Debant, S. Delaune, C. Wiedling, "Proving physical proximity using symbolic models", *in: 38th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS'18)*, *LIPIcs*, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2018, https://hal.archives-ouvertes.fr/hal-01708336.

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 typesThe 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 also improved existing decision procedures. In particular, we extended the procedure implemented in the tool AKISS to deal with the exclusive or operator [BDGK17]. We successfully used this extension on several case studies that were outside the scope of existing tools, e.g., unlinkability on various RFID protocols, and resistance against guessing attacks on protocols that use xor. Lastly, most of the existing decision procedures for checking trace equivalence rely on a naive and expensive exploration of all interleavings of concurrent actions, which calls for partial-order reduction (POR) techniques. We developed POR techniques for protocol equivalences [DBH17,DBH18]. These techniques have been integrated in existing tools such as Apte and DeepSec, and we conducted complete benchmarks showing dramatic improvements.

3.9 Establishing equivalence-based properties in the general case

Participants: Stéphanie Delaune, Solène Moreau, Vaishnavi Sundararajan.

Collaborations: David Baelde (MdC, ENS Paris Saclay), Véronique Cortier (DR CNRS, 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

[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`.

[BDGK17] D. Baelde, S. Delaune, I. Gazeau, S. Kremer, "Symbolic Verification of Privacy-Type Properties for Security Protocols with XOR", *in : CSF 2017 - 30th IEEE Computer Security Foundations Symposium*, IEEE, Santa Barbara, United States, August 2017, `https://hal.archives-ouvertes.fr/hal-01906644`.

[DBH17] S. Delaune, D. Baelde, L. Hirschi, "A Reduced Semantics for Deciding Trace Equivalence", *Logical Methods in Computer Science 13*, 2, June 2017, p. 1–48, `https://hal.archives-ouvertes.fr/hal-01906639`.

[DBH18] S. Delaune, D. Baelde, L. Hirschi, "POR for Security Protocol Equivalences - Beyond Action-Determinism", *in : Computer Security - 23rd European Symposium on Research in Computer Security*, Barcelone, Spain, 2018, `https://hal.archives-ouvertes.fr/hal-01906651`.

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). We are currently working to extend this result to the case of stateful protocols.

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.

3.10 Security Modeling with Attack–Defense Trees

Participants: Barbara Kordy, 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 2. 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.

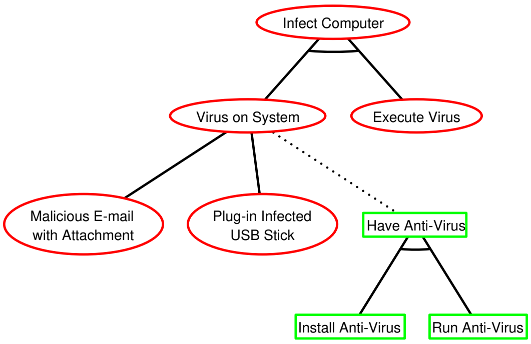


Figure 2: Attack–defense tree for infecting a computer

Recently, we have been especially interested in the following aspects of attack and defense modeling and analysis:

- The enrichment of the attack–defense tree model allowing the analysis of real security scenarios. In particular, we have developed the theoretical foundations and quantitative evaluation algorithms for the model where an attacker's action can contribute to several attacks and a countermeasure can prevent several threats [BK17,KW18].

[BK17] A. Bossuat, B. Kordy, "Evil Twins: Handling Repetitions in Attack-Defense Trees - A

- The design of a technique, using linear programming methods, for selecting an optimal set of countermeasures, taking into account the budget available for protecting the analyzed system. It is a generic technique that can be applied to several optimization problems, for example, maximizing the attack surface coverage, or maximizing the attacker's investment [KW17].
- The problem of designing an attack tree that satisfies some desired correctness properties [APK17], and that is suitable for the analysis of a specific system [APK18].

Hardware and Software Systems Security

3.11 Side-Channel Attacks

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

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

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 CCS 2016, we propose the strong non-interference security notion that allows to compose masked implementations. It is a very hard problem to check the security of masked implementation and here, we show that we can split this problem into smaller ones and use composition theorem to prove the security of larger circuits. We also propose at ESORICS 2019 a tool for verifying the security of hardware implementations against stronger attacks called glitch effect.

At CCS 2017, we propose a timing and a power analysis attack on the BLISS lattice-based signature scheme. At EUROCRYPT 2018, we propose the first secure implementation of a lattice-based signature schemes. At ASIACRYPT 2018 we used linear regression to study the Lattice With Errors over the integers problem for breaking a signature scheme using a SPA attack. At ACNS 2019, we propose to evaluate a masked implementation on the Dilithium signature scheme. At CCS 2019 we use phase retrieval algorithms to break the BLISS signature scheme. Finally, we use more recently new

Survival Guide", *in: GraMSec@CSF*, *Lecture Notes in Computer Science*, *10744*, Springer, p. 17–37, 2017.

[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.

[KW17] B. Kordy, W. Widel, "How Well Can I Secure My System?", *in: IFM*, *Lecture Notes in Computer Science*, *10510*, Springer, p. 332–347, 2017.

[APK17] M. Audinot, S. Pinchinat, B. Kordy, "Is My Attack Tree Correct?", *in: ESORICS (1)*, *Lecture Notes in Computer Science*, *10492*, Springer, p. 83–102, 2017.

[APK18] M. Audinot, S. Pinchinat, B. Kordy, "Guided Design of Attack Trees: A System-Based Approach", *in: CSF*, IEEE Computer Society, p. 61–75, 2018.

results to recover the signature key from the Gram-Schmidt of the NTRU basis in Falcon.

3.12 Symmetric Searchable Encryption

Participants: Raphaël Bost and Pierre-Alain Fouque.

Collaborations: Brice Minaud (RHUL), Olya Ohrimenko (MSR Cambridge, UK).

In this area, we propose efficient symmetric searchable encryption (SSE) schemes that allow to query an encrypted database. The idea of index solution is to encrypt for each keyword the set of indices of documents matching this keyword. The security of SQL database is a more difficult problem and recently frequence analysis have shown that range queries lead to total break of these schemes.

At CCS 2016 we propose the first forward secure scheme. This was an important result, because such schemes avoid many attacks on SSE schemes. At CCS 2017 he also proposed more efficient generic schemes and look at the backward security. At PETS 2019, we showed some tradeoff between security and efficiency of these schemes.

Raphaël received the prize of the best thesis of the GDR Security in 2019 for his thesis defended in January 2018.

3.13 Intrusion Detection using Statistical tools

Participants: Alban Siffer and Pierre-Alain Fouque.

Collaborations: Alexandre Termier (Lacodam team), Christine Largouët (Lacodam team).

We first propose two algorithms for detecting anomalies and drift in a time series. We used them to detect anomalies in stream data to detect cybersecurity attacks and we showed that previous tools using machine learning were not well-suited. We developed a new probe for detecting these attacks by monitoring simple counters. This work has been published at KDD 2017.

Then, we study the problem of testing unimodal distribution in large dimension and we develop the first efficient tools at KDD 2018. Finally, we improve this work using another test which gives more information about the modes and construct a new clustering algorithm which makes fewer calls to k-means.

Alban defended his PhD in December 2019.

3.14 Time-Memory Trade-Off (TMTO)

Participants: Gildas Avoine, Barbara Kordy, Florent Tardif.

Collaborations: UC Irvine (USA).

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 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 UC Irvine (USA) 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.

3.15 Forensics for Smartcards

Participants: Gildas Avoine, Thomas Gougeon.

Collaborations: ENSICAEN (France).

Smart cards usually gather and store personal data, possibly related to the behavior of their holder. They are typically low-cost devices including (but not limited to) credit cards, mass transportation passes, electronic passports, keyless entry and start systems, and ski passes. In most cases, the personal data contained in these devices are accessible without requiring any authentication. For example, the Mobib card contains sensitive data, including holder's name, zip code, and native language. Interpreting the meaning of the captured data is difficult and time-consuming when neither the data structure nor the data encoding are known, particularly if the number of devices is large. So far, it does not exist any adapted method to automatically retrieve information stored in these devices, whereas there is really a need for a generic method investigating these devices. This kind of investigation is involved in several scenarios: (i) to establish digital evidence in connection with criminal investigations, (ii) to retrieve information about a missing person, or (iii) to verify whether a system complies with the claims of manufacturer or authority. EMSEC developed automatic methods based on machine learning techniques to retrieve text, dates, and cryptographic material [GBL+16][GBL+17a][GBL+17b] in memory

[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.

[GBL+16] T. Gougeon, M. Barbier, P. Lacharme, G. Avoine, C. Rosenberger, "Memory dumps where neither the data structure nor the data encoding are known (see Figure 3).

```
00 00 00 00 00 00 00 04 00 71 B3 00 00 00 00 00 01 B8 B2 4A 02 50 00 33 01 1A 13 43 00
04 00 98 E5 94 C8 02 0D 60 C9 65 C7 D5 90 00 00 00 00 00 00 00 19 75 07 10 92 82 D2 CF
F3 6A 68 88 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
08 38 2B 00 08 BD 59 2A 46 60 C4 81 98 E5 94 C8 02 0D 60 C9 65 C6 41 F4 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
09 0E E5 92 04 20 60 86 60 00 00 00 00 1C D6 DD 56 40 00 01 C0 00 00 51 08 66 E0 00 00
09 0E E5 7A 04 20 60 86 60 00 00 00 00 1C D6 DD 56 40 00 01 80 00 00 11 08 66 E0 00 00
09 0E E5 5A 04 20 60 86 60 00 00 00 00 1C D6 DD 56 40 00 01 40 00 00 91 08 66 E0 00 00
11 2B 40 01 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Figure 3: Example of Memory Dump

3.16 Browser Fingerprinting

Participants: Gildas Avoine.

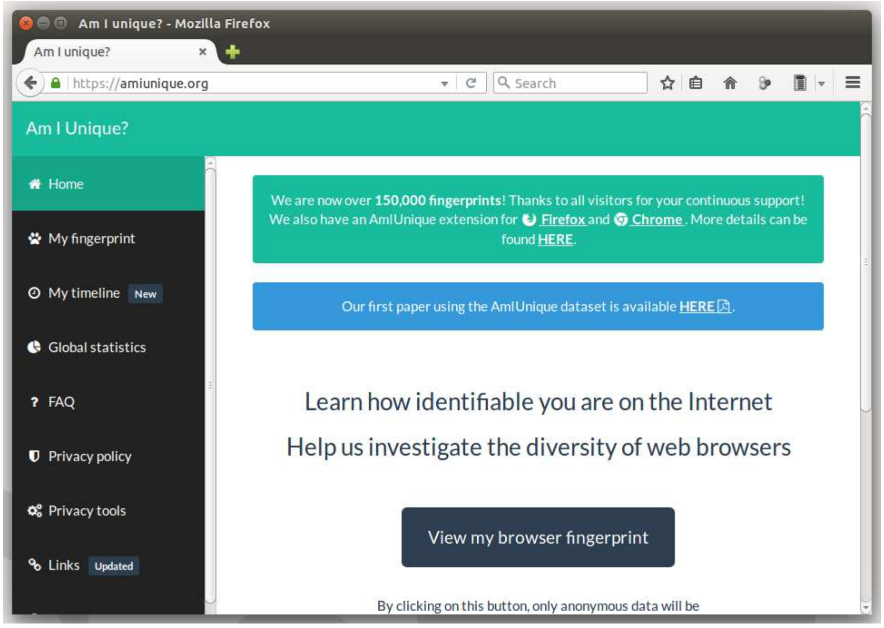
Collaborations: Pierre Laperdrix, Benoît Baudry (IRISA/DIVERSE).

Browser fingerprinting has emerged in the past few years as a strong alternative to cookie-based tracking: the collection of device-specific attributes through the browser, allows one to build a signature, which uniquely identifies a device. Yet, very few works have explored the use of browser fingerprinting for authentication and none of them have tried to quantify the provided protection. The main challenge for authentication is that most collected attributes of a browser are static (e.g., they are constant and do not depend on any input) and they can easily be modified and replayed, opening the door to attackers impersonating other devices. The key insight of this work is that canvas fingerprinting can be used for challenge/response-based authentication. EMSEC investigates this approach to strengthen the security of multifactor authentication schemes. To address this question, Pierre Laperdrix launched a website to gather browser fingerprints, known as www.amiunique.org, which is illustrated in Figure 4.

carving in embedded devices: separate the wheat from the chaff", *in : Applied Cryptography and Network Security – 14th International Conference – ACNS*, M. Manulis, A. Sadeghi, S. Schneider (editors), *LNCS*, *9696*, Springer-Verlag, p. 592–608, Guildford, UK, June 2016.

[GBL^{+}17a] T. Gougeon, M. Barbier, P. Lacharme, G. Avoine, C. Rosenberger, "Memory carving can finally unveil your embedded personal data", *in : Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES)*, Reggio di calabria, Italy, August 2017, https://hal.archives-ouvertes.fr/hal-01615205.

[GBL^{+}17b] T. Gougeon, M. Barbier, P. Lacharme, G. Avoine, C. Rosenberger, "Retrieving Dates in Smart Card Dumps is as Hard as Finding a Needle in a Haystack", *in : The IEEE Workshop on Information Forensics and Security (WIFS)*, Rennes, France, December 2017, https://hal.archives-ouvertes.fr/hal-01615218.



We are now over **150,000 fingerprints**! Thanks to all visitors for your continuous support! We also have an AmIUnique extension for Firefox and Chrome. More details can be found HERE.

Our first paper using the AmIUnique dataset is available HERE.

Learn how identifiable you are on the Internet

Help us investigate the diversity of web browsers

By clicking on this button, only anonymous data will be

Figure 4: Am I unique?

4 Software development and platforms

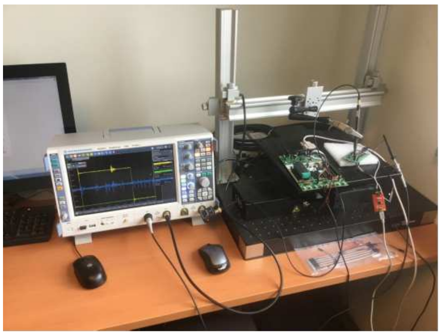
4.1 Platform "Cryptographic Computing" (PF-SP3-02)

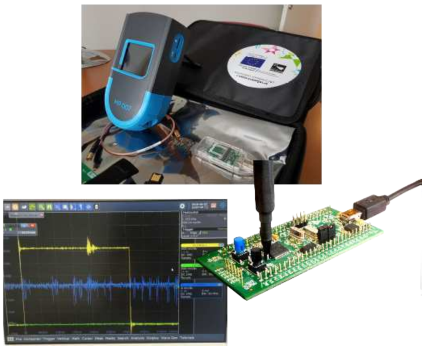
The platform PF-SP3-02 has a large computing capacity as well as a large memory capacity both in terms of storage memory and fast access memory (RAM or SSD). It indeed contains a 768-GB RAM computer, along with several medium-range servers. The plateform will be completed in 2019 with several AMD EPYC ROME (64 cores - 128 threads) computers.

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. In 2019, the platform will be 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.





The Cyber Ubiquitous Platform “Attacks on Embedded Systems” is jointly managed by Université Rennes 1 and INSA Rennes, and it is located at IRISA.

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 CRYPTACUS

- Funding: H2020 COST Action
- Hosting Institution: INSA
- Budget: 500 000 EUR
- PI: Gildas Avoine
- Period: 12/12/2014 - 11/12/2018
- URL: `https://www.cryptacus.eu`
- Description: Recent technological advances in hardware and software have irrevocably affected the classical picture of computing systems. Today, these no longer consist only of connected servers, but involve a wide range of pervasive and embedded devices, leading to the concept of "ubiquitous computing systems". The objective of the Action is to improve and adapt the existent cryptanalysis methodologies and tools to the ubiquitous computing framework. Cryptanalysis, which is the assessment of theoretical and practical cryptographic mechanisms designed to ensure security and privacy, will be implemented along four axes: cryptographic models, cryptanalysis of building blocks, hardware and software security engineering, and security assessment of real-world systems.

5.2 National Initiatives

5.2.1 ANR Brutus

- Funding: ANR
- Hosting Institution: UR1
- Budget total : 740 000 EUR
- PI: Pierre-Alain Fouque
- Period: 2014-2018
- URL: `https://anr.fr/Project-ANR-14-CE28-0015`
- Description: The Brutus project aims at investigating the security of authenticated encryption systems. It aims to evaluate carefully the security of the most promising candidates, by trying to attack the underlying primitives or to build security proofs of modes of operation. It targets the traditional black-box setting, but also more “hostile” environments, including the hardware platforms where some side-channel information is available. It also aims at quantifying the impact of not respecting implementation hypotheses such as not reusing a nonce. Finally, a more constructive goal of the Brutus project is to advise solutions in each of these scenarios, including the choice of a cryptosystem and implementation aspects. This constructive task will be extended to the field of white box cryptography, which aims at hiding the key even if the full implementation is available, including any secret data.

5.2.2 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.

5.2.3 ANR Decrypt

- Funding: ANR
- Hosting Institution: UR1
- Budget total : About 180 000 EUR
- PI: Marine Minier (Loria, Nancy)
- EMSEC: Patrick (PI local), Stéphanie, Pierre-Alain
- Period: 01/01/2019 - 31/12/2022
- URL: `https://decrypt.limos.fr/`
- Description: This project aims to propose a declarative language dedicated to cryptanalytic problems in symmetric key cryptography using constraint programming (CP) to simplify the representation of attacks, to improve existing attacks and to build new cryptographic primitives that withstand these attacks. We also want to compare the different tools that can be used to solve these problems: SAT and MILP where the constraints are homogeneous and CP where the heterogeneous constraints can allow a more complex treatment. One of the challenges of this project will be to define global constraints dedicated to the case of symmetric cryptography. Concerning constraint programming, this project will define new dedicated global constraints, will improve the underlying filtering and solution search algorithms and will propose dedicated explanations generated automatically.

5.2.4 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.

5.2.5 ANR JCJC CryptAudit

- Funding: ANR
- Hosting Institution: UR1
- Budget: About 250 000 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:

  - Extended Demirci-Selçuk Attacks on Block Ciphers. The first goal is to extend the Demirci-Selçuk attacks to new security models: the related-keys and related-tweaks settings. This will allow to apply the technique to tweakable block ciphers, compression functions and authenticated encryptions. We also plan to improve this technique against non-SPN (Substitution-Permutation Networks) ciphers as Feistel Networks.

  - Cryptanalysis of Stream Ciphers. So far there is no tool dedicated to stream ciphers and security analysis of such primitives is done by hand. Hence, many stream ciphers (e.g. FIDES, SPROUT, FLIP) were broken few time after their specifications were publicly released. For this axis, we will first focus on stream ciphers used in real world such as Snow3G, ZUC, HiTag and Chacha, with the aim of providing a tool looking for various types of attacks for each of these designs. Then we will study in priority stream ciphers used with Fully-Homomorphic Encryption and develop new cryptanalysis techniques.

- Cryptanalysis of SHA-3. SHA-3 looks more complicated than AES since it is composed of more complex operations in 3-dimensional space with longer axis (5 x 5 x 64). Consequently, it is relatively difficult to find attack by hand. Some tools have been developed by the Keccak team for discovering differential characteristics, that can lead to attack on the hash function. In this direction, our aim is to study the security of the internal permutation, since the whole security of the hash function relies on it. Studying round reduced versions is also of interests since such versions are used for the Ketje and Keyak authenticated encryption schemes.

- Computer-aided Conception of Symmetric Primitives. For this axis we want to use tools from above axis and to develop new ones to design a new lightweight stream ciphers well-adapted to 5G requirements and to lead researches on the design of key schedules.

5.2.6 CNRS: FCS (PICS)

- Title: *Foundation of cybersecurity scripts*
- Funding: CNRS
- Hosting Institution: CNRS
- Budget: 4 000 EUR / an
- PI: Barbara Kordy
- 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 and the Computing, School of Science and Engineering from the University of Dundee in Scotland.

5.2.7 BPI: RISQ

- Funding: BPI
- Hosting Institution: UR1
- Budget: 270 000 EUR
- PI: Philippe Nguyen (Secure-IC)
- EMSEC: Pierre-Alain, Adeline, Paul, Adela
- 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.

5.2.8 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.

5.2.9 CPER

- Funding: UE, Région, Départ., Métropole, etc.
- PI EMSEC: Pierre-Alain Fouque et Gildas Avoine
- Hosting Institution: 65 000 EUR UR1 and 200 000 EUR INSA Rennes
- Period: 2015 - 2020
- Description: The CPER SSI (Contrat de plan État-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

- PhD thesis DGA-MI, Raphaël Bost
  Pierre-Alain Fouque co-supervises the PhD thesis of Raphaël Bost with David Pointcheval on Cloud security. They have propose to add integrity of the Symmetric Searchable Encryption schemes. Since many attacks have been recently propose on provable schemes, they have tried to understand what was wrong in the security model. They understand some mistakes and they propose to fix the definition and prove the security of some scheme. Raphaël receives the price of the best PhD of the GDR Security in May 2019.
- 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, 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 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

- Barbara visited the LAAS laboratory in Toulouse on 11–12 January 2017.

- Barbara visited the University of Luxembourg (Luxembourg) on 9–10 November 2017.

- Patrick visited the Chinese Academy of Sciences on 13–20 May 2017.

5.4.2 Visiting researchers

- Mehdi Tibouchi from NTT Japan visited P.-A. Fouque in 2017.

- Florian Kammüller from the Middlesex University London, UK, visited Barbara Kordy on 8–10 February 2017.

- Rolando Trujillo Rasúa from the University of Luxembourg (Luxembourg) visited Gildas Avoine and Barbara Kordy on 13–23 February 2017.

6 Dissemination

6.1 Promoting scientific activities

- Gildas Avoine is a member of the *Institut Universitaire de France*. He also is the director of the CNRS' GDR (national scientific network) in computer security (1000+ researchers), the chair of the COST Action IC1403 (Cryptacus), and a member of the steering committee of the "Défi 9" of the ANR (French funding agency). He belongs to the cybersecurity workgroup of Allistene (*Alliance des sciences et technologies du numérique*). He was in 2017 a member of evaluation committees for the European Research Council, the Swiss National Science Foundation, and the H2020 COST Association.

- 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 the PI for the ANR Brutus and ANR SafeTLS projects. He participated to the Dagstuhl seminar on Public-Key Cryptography in September 2017. He was a member of the FSE, MathCrypt, CHES program committees. He was one of the designer of the Falcon lattice-based signature scheme presented to the NIST post-quantum competition. He was also one of the organizers of a workshop on Quantum and Post-Quantum cryptography in April 2017 at Sorbonne University.

- Stéphanie Delaune is the PI of the ERC Starting Grant POPSTAR (2017-2022). She was a member of the POST, CSR, CADE, CSF, and FST&TCS program committees in 2017. 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. 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 member of the scientific council of the GDR-IM. She was elected to the laboratory council at IRISA in 2017.

- Clémentine Maurice joined the team in October 2017. She was a member of the ACSAC and ESSoS program committees. She gave an invited presentation at the Cryptacus Workshop in Nijmegen.

- Patrick Derbez is the PI of the JCJC ANR project CryptAudit and involved in the ANR project BRUTUS. He is a PC member of ToSC IACR journal. He was an invited speaker at ASK'17 (Asian Symmetric Workshop) and led a working group during the workshop. He also visited the Chinese Academy of Sciences in May 2017 and gave a talk at the University of Beijing.

- In 2017, Barbara Kordy was a PC member of the CRiSIS'17 conference (https://conferences.telecom-bretagne.eu/crisis/2017/). She reviewed for CSF'17, CRiSIS'17, GraMSec'17, and the Elsevier's *Computer Science Review* journal. Barbara was a member of the the selection committee for an assistant professor (MCF) position at IUT Limoges. Finally, 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 was a member of the scientific committee 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 "Journée C2" (annual event of the GT-C2). She was a PC member of the Indrocrypt conference.

6.2 Teaching and Juries

6.2.1 Teaching

- Gildas Avoine is in charge of two 10-hour courses "Network Security" (4th-year students in computer science, and in telecommunication) and the 26-hour course "Cryptographic Engineering" (4th-year students) both at INSA Rennes. He also teaches "Advanced Security" at the UCL Belgium.
- Stéphanie Delaune co-lectures (with Barbara Kordy) 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).
- Patrick Derbez is in charge of a 48-hour course "Algorithms for Security" (4th-year students) and of a 10-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.
- Barbara Kordy lectures and is in charge of the 32-hour course "Languages and grammars" (4th-year students, INSA Rennes), the 24-hour course "Security" (5th-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 was in charge of a group of 5th-year students in the lecture "Veille Technologique" at Rennes University.
- Adeline Roux-Langlois was in charge of a 24-hour course on "Introduction to Cryptography" (1st year students at ENS Rennes) and co-lecture 24 hours in a 32-hour course "Lattices for cryptography" (5th year students, UR1).

6.2.2 PhD and HDR Juries

- Han Qiu, Telecom ParisTech, November 2017 (Gildas Avoine was "rapporteur")
- Anna Krasnova, Radboud University Nijmegen, October 2017 (Gildas Avoine was "rapporteur")
- Sonia Mihaela Bogos, EPFL, Switzerland, May 2017 (P.-A. Fouque was "rapporteur")
- Maria Naya-Plasencia (HDR), INRIA, May 2017 (P.-A. Fouque was "Member")

- Margaux Dugardin, Telecom ParisTech, May 2017 (P.-A. Fouque was "rapporteur")
- Alvaro Garcia Recuero, Rennes, May 2017 (P.-A. Fouque was "Member")
- Solenn Bunet, Rennes, November 2017 (P.-A. Fouque was "President")
- Chrysanthi Mavromati, UPMC, January 2017 (P.-A. Fouque was "Member")
- Céline Chevalier (HDR), ENS Paris, December 2017 (Stéphanie Delaune was "Member")
- Florian Bourse, ENS Paris, Decembre 2017 (Adeline Roux-Langlois was "Member")

6.3 Popularization

- Gildas Avoine is the author (jointly with Marc-Olivier Killijian) of an article "Cybersecurity" published in the journal *1024* of the SIF (*Société informatique de France*).
- Gildas Avoine and Thomas Gougeon are the authors of the article "Investigation numérique dans votre porte-feuille" published in the journal *MISC Issue HS15* (*Multi-System & Internet Security Cookbook*).
- Gildas Avoine, Barbara Kordy, and Florent Tardif are the authors of the article "Cassage de mots de passe : que mettre dans votre boite à outils ?" published in the journal *MISC Issue 89* (*Multi-System & Internet Security Cookbook*).
- Gildas Avoine was invited to the radio show "Autour de la question" (Radio France International) on January 19th, 2017.
- Patrick Derbez introduced research in cryptography to high school students during "Immersion Sciences", an event organized by "Region Bretagne" to promote sciences.

7 Bibliography

Articles in referred journals and book chapters

[1] V. Cheval, H. Comon-Lundh, S. Delaune, "A procedure for deciding symbolic equivalence between sets of constraint systems", *Information and Computation 255*, August 2017, p. 94 – 125, https://hal.archives-ouvertes.fr/hal-01906636.

[2] V. Cheval, H. Comon-Lundh, S. Delaune, "A procedure for deciding symbolic equivalence between sets of constraint systems", *Information and Computation 255*, August 2017, p. 94 – 125, https://hal.inria.fr/hal-01584242.

[3] S. Delaune, D. Baelde, L. Hirschi, "A Reduced Semantics for Deciding Trace Equivalence", *Logical Methods in Computer Science 13*, 2, June 2017, p. 1–48, https://hal.archives-ouvertes.fr/hal-01906639.

[4] S. Delaune, L. Hirschi, "A survey of symbolic methods for establishing equivalence-based properties in cryptographic protocols", *Journal of Logical and Algebraic Methods in Programming 87*, February 2017, p. 127 – 144, https://hal.archives-ouvertes.fr/hal-01906634.

Publications in Conferences and Workshops

[5] M. Audinot, S. Pinchinat, B. Kordy, "Is my attack tree correct?", *in: ESORICS 2017 - 22nd European Symposium on Research in Computer Security, European Symposium on Research in Computer Security : Computer Security – ESORICS 2017, 10492*, Springer, p. 83–102, Oslo, Norway, September 2017, https://hal.inria.fr/hal-01686505.

[6] G. Avoine, X. Bultel, S. Gambs, D. Gerault, P. Lafourcade, C. Onete, J.-M. Robert, "A Terrorist-fraud Resistant and Extractor-free Anonymous Distance-bounding Protocol", *in: ACM Symposium on Information, Computer and Communications Security (AsiaCCS 2017)*, ACM, p. 800–814, Abu Dhabi, United Arab Emirates, April 2017, https://hal.archives-ouvertes.fr/hal-01588560.

[7] G. Avoine, X. Carpent, "Heterogeneous Rainbow Table Widths Provide Faster Cryptanalyses", *in: Asia Conference on Computer and Communications Security, AsiaCCS 2017, Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, AsiaCCS 2017, Abu Dhabi, United Arab Emirates, April 2-6, 2017*, ACM Press, Abu Dhabi, United Arab Emirates, April 2017, https://hal.archives-ouvertes.fr/hal-01689103.

[8] D. Baelde, S. Delaune, I. Gazeau, S. Kremer, "Symbolic verification of privacy-type properties for security protocols with XOR", *in: CSF 2017 - 30th IEEE Computer Security Foundations Symposium*, p. 15, Santa Barbara, United States, August 2017, https://hal.inria.fr/hal-01533708.

[9] D. Baelde, S. Delaune, I. Gazeau, S. Kremer, "Symbolic Verification of Privacy-Type Properties for Security Protocols with XOR", *in: CSF 2017 - 30th IEEE Computer Security Foundations Symposium*, IEEE, Santa Barbara, United States, August 2017, https://hal.archives-ouvertes.fr/hal-01906644.

[10] J.-F. Biasse, T. Espitau, P.-A. Fouque, A. Gélin, P. Kirchner, "Computing generator in cyclotomic integer rings", *in: 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2017), Lecture*

Notes in Computer Science, *10210*, p. 60–88, Paris, France, April 2017, https://hal.archives-ouvertes.fr/hal-01518438.

[11] G. Bonnoron, C. Fontaine, G. Gogniat, V. Herbert, V. Lapotre, V. Migliore, A. Roux-Langlois, "Somewhat/Fully Homomorphic Encryption: Implementation Progresses and Challenges", *in: C2SI 2017 : 2nd International Conference on Codes, Cryptology and Information Security, 10194 - LNCS (Lectures Notes in Computer Science)*, Springer, p. 68 – 82, Rabat, Morocco, April 2017, https://hal.archives-ouvertes.fr/hal-01596540.

[12] A. Bossuat, B. Kordy, "Evil Twins: Handling Repetitions in Attack–Defense Trees: A Survival Guide", *in: Graphical Models for Security*, P. Liu, S. Mauw, , K. Stolen (editors), *LNCS*, 10744, Springer, p. 17–37, Santa Barbara, United States, August 2017, https://hal.inria.fr/hal-01728782.

[13] C. Bouillaguet, C. Delaplace, P.-A. Fouque, P. Kirchner, "Fast Lattice-Based Encryption: Stretching Spring", *in: International Workshop on Post-Quantum Cryptography*, Utrecht, Netherlands, June 2017, https://hal.inria.fr/hal-01654408.

[14] I. Boureanu, D. Gerault, P. Lafourcade, C. Onete, "Breaking and fixing the HB+DB protocol", *in: Wisec 2017 - Conference on Security and Privacy in Wireless and Mobile Networks*, p. 241 – 246, Boston, United States, July 2017, https://hal.archives-ouvertes.fr/hal-01588562.

[15] 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.

[16] V. Cortier, A. Dallon, S. Delaune, "SAT-Equiv: An Efficient Tool for Equivalence Properties", *in: 30th IEEE Computer Security Foundations Symposium (CSF'17)*, p. 481 – 494, Santa Barbara, United States, July 2017, https://hal.inria.fr/hal-01624274.

[17] S. Delaune, S. Kremer, L. Robin, "Formal verification of protocols based on short authenticated strings", *in: CSF 2017 - 30th IEEE Computer Security Foundations Symposium*, IEEE (editor), p. 14, Santa Barbara, United States, August 2017, https://hal.inria.fr/hal-01528607.

[18] S. Delaune, S. Kremer, L. Robin, "Formal Verification of Protocols Based on Short Authenticated Strings", *in: 2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, IEEE, Santa Barbara, France, August 2017, https://hal.archives-ouvertes.fr/hal-01906646.

[19] T. Espitau, P.-A. Fouque, B. Gérard, M. Tibouchi, "Side-Channel Attacks on BLISS Lattice-Based Signatures", *in: 2017 ACM Conference on Computer and Communications Security (CCS 2017)*, ACM, p. 1857–1874, Dallas, TX, United States, October 2017, https://hal.sorbonne-universite.fr/hal-01648080.

[20] T. Gougeon, M. Barbier, P. Lacharme, G. Avoine, C. Rosenberger, "Memory carving can finally unveil your embedded personal data", *in: Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES)*, Reggio di calabria, Italy, August 2017, https://hal.archives-ouvertes.fr/hal-01615205.

[21] T. Gougeon, M. Barbier, P. Lacharme, G. Avoine, C. Rosenberger, "Retrieving Dates in Smart Card Dumps is as Hard as Finding a Needle in a Haystack", *in: The IEEE Workshop on Information Forensics and Security (WIFS)*, Rennes, France, December 2017, https://hal.archives-ouvertes.fr/hal-01615218.

[22] B. Libert, T. Peters, C. Qian, “Structure-Preserving Chosen-Ciphertext Security with Shorter Verifiable Ciphertexts”, *in: PKC 2017 - Public Key Cryptography, LNCS, 10174*, Springer, p. 247 – 276, Amsterdam, Netherlands, March 2017, `https://hal.inria.fr/hal-01621022`.

[23] A. Siffer, P.-A. Fouque, A. Termier, C. Largouët, “Anomaly Detection in Streams with Extreme Value Theory”, *in: KDD 2017 - Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Halifax, Canada, August 2017, `https://hal.archives-ouvertes.fr/hal-01640325`.

[24] 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`.

[25] W. Widel, B. Kordy, “How well can I secure my system?”, *in: 13th International Conference on integrated Formal Methods (iFM 2017)*, Turin, France, September 2017, `https://hal.archives-ouvertes.fr/hal-01580990`.

Miscellaneous

[26] G. Avoine, B. Bignon, B. Kordy, F. Tardif, “Cassage de mots de passe : que mettre dans votre boîte à outils ?”, Editions Diamond, 2017, Science popularization, `https://hal.archives-ouvertes.fr/hal-01492840`.

[27] G. Avoine, M.-O. Killijian, “Cybersécurité”, October 2017, Bulletin de la société informatique de France, `https://hal.archives-ouvertes.fr/hal-02182937`.