UMR IRISA

Activity Report 2021

Team CAPSULE

Applied Cryptography & Implementation Security

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

Patrick Derbez	Assistant Professor	Univ. Rennes 1
Pierre-Alain Fouque (*)	Professor	Univ. Rennes 1
Annelie Heuser	Junior Researcher	CNRS
Adeline Roux-Langlois	Junior Researcher, HDR	CNRS
Alexandre Wallet	Junior Researcher	Inria

(*) Leader

PhD students

Olivier Bernard	Feb 2019 to Jan 2022	Thales + H2020 Prometheus
Christophe Genevey-Metat	Sep 2018 to Aug 2021	DGA
Arthur Gontier	Sep 2020 to Aug 2023	ANR Decrypt
Corentin Jeudy	Sep 2021 to Aug 2024	Orange Labs
Hoa Nguyen	Sep 2021 to Aug 2024	DGA
Thi-Thu Quyen Nguyen	Sep 2021 to Aug 2024	Idemia
Paul Kirchner	Mar 2018 to Mar 2021	BPI RISQ + DGA
Duy-Phuc Pham	Sep 2019 to Aug 2022	ANR AHMA
Lucas Prabel	Sep 2020 to Aug 2023	DGA
Agathe Cheriere	Sep 2020 to Aug 2023	DGA

Daniel Braga de Almeida (DGA, advisors: P.A. Fouque, 50%, M. Sabt, 50%, 2019-2022) and Gwendal Patat (UR1, advisors: P.A. Fouque, 50% M. Sabt, 50 %, 2020-2023) will be in the Spicy team.

Postdocs

Scientific collaborators (including post-docs, engineers):

Nicolas Aragon	Sep 2021 to Aug 2022	ANR IDROMEL
Alexandre Gonzalvez	Sep 2021 to Oct 20222	DGA
Ronan Lashermes	Sep 2020	Inria engineer
Andréa Lesavourey	June 2021 to Sep 2022	DGA SAD
Damien Marion	Sep 2021 to Oct 2023	ANR AHMA

Associate members

Benoît Gérard	Sep 2013 to Oct 2022	DGA-MI
Tuong-Huy Nguyen	Sep 2020 to Aug 2022	DGA-MI
Julien Devigne	Sep 2019 to Aug 2022	DGA-MI

Administrative assistant

Hélène De La Ruée

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 CAPSULE work on different aspects of cryptology, in particular on lattice-based cryptography, symmetric cryptanalysis, and security of protocols. CAPSULE is also strongly involved in two important NIST competitions about the security of post-quantum schemes and lightweight ciphers. CAPSULE 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 side channels. Finally, CAPSULE considers various topics related to the use of cryptography in real-world systems and to malware analysis.

2.2 Scientific foundations

CAPSULE's research activities are organized along four axes, namely symmetric-key cryptography, post-quantum cryptography, security of cryptographic hardware and software implementations, and the real-world cryptographic systems. We add an item this year around Malware Analysis since some works have been done in this direction.

- Design and analysis of ciphers: lightweight block ciphers, authenticated encryption schemes, etc.
- Lattice-based cryptography, security proofs and advanced constructions
- Security of cryptographic implementations: side-channel attacks, micro-architectural attacks and countermeasures
- Design and analysis of real-world cryptographic systems such as WhatsApp and Signal secure messaging or database security with Searchable Symmetric Encryption Schemes.

2.3 Highlight Results of 2021

1. We wrote a new project team for Capsule between IRISA and Inria. This project has been evaluation by Alain Girault, responsible for the theme "Algorithm" at Inria. The next step will be the evaluation by 2 experts. However, CNRS did not answer to Inria in June. In September, we begin to create a new team at IRISA, that was created by the end of 2021.

2. Patrick's work on GPRS encryption scheme received a world-wide audience `https://www.schneier.com/blog/archives/2021/06/intentional-flaw-in-gprs-encryption-algorithm-gea-1.html`

3. Annelie's work published at ACSAC has been reported in many websites (see popularization results section).

3 Scientific achievements

Axis "Symmetric-Key Cryptography"

3.1 Symmetric Cryptography

Participants: Patrick Derbez and Pierre-Alain Fouque.

Collaborations: LORIA (Nancy), INRIA (Paris), EMN (Nantes), Bochum.

Symmetric Key Cryptography also known as Symmetric Encryption is when a secret key is leveraged for both encryption and decryption functions. This method is the opposite of Asymmetric Encryption where one key is used to encrypt and another is used to decrypt. During this process, data is converted to a format that cannot be read or inspected by anyone who does not have the secret key that was used to encrypt it.

At Rennes, we are experts in cryptanalysis of block ciphers, stream ciphers, and hash funnctions. We build specific tools for looking automatically for the best attacks. Nowadays, we use more and more MILP or Constrained Programming Tools with the Choco team at Nantes.

Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2
Authors: Christof Beierle, Patrick Derbez, Gregor Leander, Gaëtan Leurent, Håvard Raddum, Yann Rotella, David Rupprecht, Lukas Stennes
Venue: EUROCRYPT 2021

Abstract: This paper presents the first publicly available cryptanalytic attacks on the GEA-1 and GEA-2 algorithms. Instead of providing full 64-bit security, we show that the initial state of GEA-1 can be recovered from as little as 65 bits of known keystream (with at least 24 bits coming from one frame) in time 2^{40} GEA-1 evaluations and using 44.5 GiB of memory.

The attack on GEA-1 is based on an exceptional interaction of the deployed LFSRs and the key initialization, which is highly unlikely to occur by chance. This unusual pattern indicates that the weakness is intentionally hidden to limit the security level to 40 bit by design.

In contrast, for GEA-2 we did not discover the same intentional weakness. However, using a combination of algebraic techniques and list merging algorithms we are still able to break GEA-2 in time $2^{45.1}$ GEA-2 evaluations. The main practical hurdle is the required knowledge of 1600 bytes of keystream.

Efficient Methods to Search for Best Differential Characteristics on SKINNY
Authors: Stéphanie Delaune, Patrick Derbez, Paul Huynh, Marine Minier, Victor Mollimard, Charles Prud'homme
Venue: ACNS 2021

Abstract: Evaluating resistance of ciphers against differential cryptanalysis is essential to define the number of rounds of new designs and to mount attacks derived from differential cryptanalysis.

In this paper, we propose automatic tools to find the best differential characteristics on the SKINNY block cipher. As usually done in the literature, we split this search in two stages denoted by Step 1 and Step 2. In Step 1, we aim at finding all truncated differential characteristics with a low enough number of active Sboxes. Then, in Step 2, we try to instantiate each difference value while maximizing the overall differential characteristic probability. We solve Step 1 using an ad-hoc method inspired from the work of Fouque et al. whereas Step 2 is modelized for the Choco-solver library as it seems to outperform all previous methods on this stage.

Notably, for SKINNY-128 in the SK model and for 13 rounds, we retrieve the results of Abdelkhalek et al. within a few seconds (to compare with 16 days) and we provide, for the first time, the best differential related-tweakey characteristics up to 14 rounds for the TK1 model. Regarding the TK2 and the TK3 models, we were not able to test all the solutions Step 1, and thus the differential characteristics we found up to 16 and 17 rounds are not necessarily optimal.

Axis "Lattice-Based Cryptography"

3.2 Lattice-based cryptography

Participants: Adeline Roux-Langlois, Pierre-Alain Fouque, Weiqiang Wen, Andrea Lesavourey, Paul Kirchner, Katharina Boudgoust, Lucas Prabel, Olivier Bernard, Corentin Jeudy, Guillaume Kaim, Alexandre Wallet.

Collaborations: Thomas Espitau (NTT), Mehdi Tibouchi (NTT), Sébastien Canard (Orange Labs), Jacques Traoré (Orange Labs).

Lattice-based cryptography regroups the approaches which consist in building cryptographic constructions and protocols with their security relying on hard problems on lattices. A lattice is defined as a set of all integer linear combinations of some linearly independent vectors that we call a basis. The lattice-based approach to build cryptographic schemes is very promising as we can observe in the ongoing NIST competition for post-quantum cryptography[1]. Indeed, lattice-based cryptography seems to be an

[1] `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography`

interesting candidate to obtain constructions which resist to attacks using a quantum computer. Since the work of Shor in 1997, the hardness of number theoretical assumptions, which are used as security foundations for many primitives, is extremely reduced when facing a quantum computer. Even if powerful enough quantum computers do not exist yet, it is necessary to be prepared and anticipate their arrival. Over the initial 69 submissions made at the NIST post-quantum competition in 2017, it is worth noticing that 5 over the 7 finalists are related to lattices: the three public key encryption schemes are CRYSTALS-Kyber, NTRU and SABER, and the two signature schemes are CRYSTALS-Dilithium and FALCON.

Our work in this area is following different directions: first we study the hardness of the underlying problems used to show the security of the constructions, both by studying algorithm to solve them and by proving they are hard under some conditions. Second, we work on the lattice-based constructions, both by building new constructions and study their concrete security.

Towards Faster Polynomial-Time Lattice Reduction
Authors: Paul Kirchner, Thomas Espitau, Pierre-Alain Fouque
Venue: CRYPTO 2021

Abstract: The LLL algorithm is a polynomial-time algorithm for reducing d-dimensional lattice with exponential approximation factor. Currently, the most efficient variant of LLL, by Neumaier and Stehlé, has a theoretical running time in $d^4B^{1+o(1)}$ where B is the bitlength of the entries, but has never been implemented. This work introduces new asymptotically fast, parallel, yet heuristic, reduction algorithms with their optimized implementations. Our algorithms are recursive and fully exploit fast matrix multiplication. We experimentally demonstrate that by carefully controlling the floating-point precision during the recursion steps, we can reduce euclidean lattices of rank d in time $\tilde{O}(d^\omega \cdot C)$, i.e., almost a constant number of matrix multiplications, where ω is the exponent of matrix multiplication and C is the log of the condition number of the matrix. For cryptographic applications, C is close to B, while it can be up to d times larger in the worst case. It improves the running-time of the state-of-the-art implementation fplll by a multiplicative factor of order $d^2 \cdot B$. Further, we show that we can reduce structured lattices, the so-called knapsack lattices, in time $\tilde{O}(d^{\omega-1} \cdot C)$ with a progressive reduction strategy. Besides allowing reducing huge lattices, our implementation can break several instances of Fully Homomorphic Encryption schemes based on large integers in dimension 2,230 with 4 millions of bits.

On the Hardness of Module-LWE with Binary Secret
Authors: Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, Weiqiang Wen
Venue: CT-RSA 2021

Abstract: We prove that the Module Learning With Errors (M-LWE) problem with binary secrets and rank d is at least as hard as the standard version of M-LWE with

uniform secret and rank k, where the rank increases from k to $d \geq (k+1)\log_2 q + \omega(\log_2 n)$, and the Gaussian noise from α to $\beta = \alpha \cdot \Theta(n^2\sqrt{d})$, where n is the ring degree and q the modulus. Our work improves on the recent work by Boudgoust et al. in 2020 by a factor of $\sqrt{md}$ in the Gaussian noise, where m is the number of given M-LWE samples, when q fulfills some number-theoretic requirements. We use a different approach than Boudgoust et al. to achieve this hardness result by adapting the previous work from Brakerski et al. in 2013 for the Learning With Errors problem to the module setting. The proof applies to cyclotomic fields, but most results hold for a larger class of number fields, and may be of independent interest.

Post-quantum Online Voting Scheme
Authors: Guillaume Kaim, Sébastien Canard, Adeline Roux-Langlois, Jacques Traoré
Venue: Financial Crypto 2021

Abstract: We propose a new post-quantum online voting scheme whose security relies on lattice assumptions. Compared to the state-of-the-art, our work does not make use of homomorphic primitives nor mix-nets, that are more traditional ways to build electronic voting protocols. The main reason is that zero-knowledge proofs, mandatory in the two aforementioned frameworks, are far to be as efficient as in classical cryptography, leading us to explore other approaches.

We rather base our work on a framework introduced by Fujioka et al. at Auscrypt 1992 that makes use of a blind signature scheme as the main building block. We depart however from this seminal work by allowing threshold issuance of blind signatures (to prevent ballot stuffing by malicious authorities) and by using a threshold post-quantum public key encryption scheme (rather than a commitment scheme) to allow voters to "vote and go" and to prevent "partial results". We instantiate all the required primitives with lattice-based constructions leading to the first online voting scheme that simultaneously provides post-quantum public verifiability and everlasting privacy (information-theoretic ballot anonymity). Another advantage of our protocol is that it can, contrary to recent proposals, efficiently handle elections with multiple candidates or with complex ballots (and not only referendums or single member plurality voting) without weakening the whole voting protocol by increasing the parameters size as with previous post-quantum voting schemes.

Implementation of Lattice Trapdoors on Modules and Applications
Authors: Pauline Bert, Gautier Eberhart, Lucas Prabel, Adeline Roux-Langlois, Mohamed Sabt
Venue: PQCrypto 2021

Abstract: We develop and implement 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 such as identity-based encryption. In particular, it is easy to use in the ring or module setting, and to modify the arithmetic on $\mathcal{R}_q$ (as different schemes have different conditions on q).

Relying on these tools, we also present 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 presented in Bert et al. in 2018. For that last scheme, we address a security issue and correct obsolescence problems in their implementation by building ours from scratch. To the best of our knowledge, this is the first efficient implementation of a lattice-based signature scheme in the standard model. Relying on that last signature, we also present the implementation of a standard model IBE in the module setting. We show that while the resulting schemes may not be competitive with the most efficient NIST candidates, they are practical and run on a standard laptop in acceptable time, which paves the way for practical advanced trapdoor-based constructions.

One Bit is All It Takes: A Devastating Timing Attack on BLISS's Non-Constant Time Sign Flips
Authors: Mehdi Tibouchi, Alexandre Wallet
Venue: J. Math. Cryptology 2021

Abstract: As one of the most efficient lattice-based signature schemes, and one of the only ones to have seen deployment beyond an academic setting (e.g., as part of the VPN software suite strongSwan), BLISS has attracted a significant amount of attention in terms of its implementation security, and side-channel vulnerabilities of several parts of its signing algorithm have been identified in previous works. In this paper, we present an even simpler timing attack against it. The bimodal Gaussian distribution that BLISS is named after is achieved using a random sign flip during signature generation, and neither the original implementation of BLISS nor strongSwan ensure that this sign flip is carried out in constant time. It is therefore possible to recover the corresponding sign through side-channel leakage (using, e.g., cache attacks or branch tracing). We show that obtaining this single bit of leakage (for a moderate number of signatures) is in fact sufficient for a full key recovery attack. The recovery is carried out using a maximum likelihood estimation on the space of parameters, which can be seen as a statistical manifold. The analysis of the attack thus reduces to the computation of the Fisher information metric.

Axis "Security of Cryptographic Implementation"

3.3 Security of Cryptographic Implementations

Participants: Pierre-Alain Fouque, Annelie Heuser, Ronan Lashermes, Benoît Gérard, Damien Marion, Alexandre Gonzalvez.

Collaborations: Spicy (Rennes), DGA–MI, ANSSI.

In computer security, a side-channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs). Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited.

In Rennes, we are interested in electromagnetic emission on embedded devices, and cache attacks on microarchitecture. We have also capabilities to perform real attacks on these systems.

PARASITE: PAssword Recovery Attack against Srp Implementations in ThE wild
Authors: Daniel Braga de Alemida, Pierre-Alain Fouque and Mohamed Sabt
Venue: CCS 2021

Abstract: Protocols for password-based authenticated key exchange (PAKE) allow two users sharing only a short, low-entropy password to establish a secure session with a cryptographically strong key. The challenge in designing such protocols is that they must resist offline dictionary attacks in which an attacker exhaustively enumerates the dictionary of likely passwords in an attempt to match the used password. In this paper, we study the resilience of one particular PAKE against these attacks. Indeed, we focus on the Secure Remote Password (SRP) protocol that was designed by T. Wu in 1998. Despite its lack of formal security proof, SRP has become a de-facto standard. For more than 20 years, many projects have turned towards SRP for their authentication solution, thanks to the availability of open-source implementations with no restrictive licenses. Of particular interest, we mention the Stanford reference implementation (in C and Java) and the OpenSSL one (in C). In this paper, we analyze the security of the SRP implementation inside the OpenSSL library. In particular, we identify that this implementation is vulnerable to offline dictionary attacks. Indeed, we exploit a call for a function computing modular exponentiation of big numbers in OpenSSL. In the SRP protocol, this function leads to the call of a non-constant time function, thereby leaking some information about the used password when leveraging cache-based Flush+Reload timing attack. Then, we show that our attack is practical, since it only requires one single trace, despite the noise of cache measurements. In addition, the attack is quite efficient as the reduction of some common dictionaries is very fast using modern resources at negligible cost. We also prove that the scope of our vulnerability is not only limited to OpenSSL, since many other projects, including Stanford's, ProtonMail and Apple Homekit, rely on OpenSSL, which makes them vulnerable. We find that our flaw might also impact projects written in Python, Erlang, JavaScript and Ruby, as long as they load the OpenSSL dynamic library for their big number operations. We disclosed our attack to OpenSSL who acknowledged the attack and timely fixed the vulnerability.

Train or Adapt a Deeply Learned Profile?
Authors: Christophe Genevey-Metat, Annelie Heuser, Benoît Gérard
Venue: Latincrypt 2021

Abstract: In recent years, many papers have shown that deep learning can be beneficial for profiled side-channel analysis. However, to obtain good performance with deep learning, an evaluator or an attacker face the issue of data. Due to the context, he might be limited in the amount of data for training. This can be mitigated with classical Machine Learning (ML) techniques such as data augmentation. However, these mitigation techniques lead to a significant increase in the training time; first, by augmenting the data and second, by increasing the time to perform the learning of the neural network.

Recently, weight initialization techniques using specific probability distributions have shown some impact on the training performances in side-channel analysis. In this work, we investigate the advantage of using weights initialized from a previous training of a network in some different contexts. The idea behind this is that different side-channel attacks share common points in the sense that part of the network has to understand the link between power/electromagnetic signals and the corresponding intermediate variable. This approach is known as Transfer Learning (TL) in the Deep Learning (DL) literature and has shown its usefulness in various domains. We present various experiments showing the relevance and advantage of starting with a pre-trained model. In our scenarios, pre-trained models are trained on different probe positions/channels/chips. Using TL, we obtain better accuracy and/or training speed for a fixed amount of training data from the target device.

Trace-to-trace translation for SCA
Authors: Christophe Genevey-Metat, Annelie Heuser, Benoît Gérard
Venue: CARDIS 2021

Abstract: Neural Networks (NN) have been built to solve universal function approximation problems. Some architectures as Convolutional Neural Networks (CNN) are dedicated to classification in the context of image distortion. They have naturally been considered in the community to perform side-channel attacks showing reasonably good results on trace sets exposing time misalignment. However, even in settings where these timing distortions are not present, NN have produced better results than legacy attacks. Recently in TCHES 2020, auto-encoders have been used as preprocessing for noise reduction. The main idea is to train an auto-encoder using as inputs noisy traces and less noisy traces so that the auto-encoder is able to remove part of the noise in the attack dataset. We propose to extend this idea of using NN for pre-processing by not only considering the noise-reduction but to translate data between two side-channel domains. In a nutshell, clean (or less noisy) traces may not be available to an attacker, but similar traces that are easier to attack may be obtainable. Availability of such traces can be leveraged to learn how to translate difficult traces to easy ones to increase attackability.

Electromagnetic fault injection against a complex CPU, toward new micro-architectural fault models
Authors: Thomas Trouchkine, Sébanjila Kevin Bukasa, Mathieu Escouteloup, Ronan Lashermes, Guillaume Bouffard
Venue: J. Cryptographic Engineering 2021

Abstract: The last years have seen the emergence of fault attacks targeting modern central processing units (CPUs). These attacks are analyzed at a very high abstraction level and, due to the modern CPUs complexity, the underlying fault effect is usually unknown. Recently, a few articles have focused on characterizing faults on modern CPUs. In this article, we focus on the electromagnetic fault injection (EMFI) characterization on a bare-metal implementation. With this approach, we discover and understand new effects on micro-architectural subsystems. We target the BCM2837 where we successfully demonstrate persistent faults on L1 instruction cache, L1 data cache and L2 cache. We also show that faults can corrupt the memory management unit (MMU). To validate our fault model, we realize a persistent fault analysis to retrieve an AES key.

Axis "Real-World Cryptography"

3.4 Real-World Cryptography

Participants: Pierre-Alain Fouque, Céline Duguey, and Adina Nedelcu.

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

Real World Cryptography aims at bringing together cryptography researchers with developers implementing cryptography in real-world systems.

At Rennes, we worked in 2021 on the security of databases using symmetric searchable encryption, on lawful interception for telecom operators, and on the security of Messaging Layer Security (MLS).

SSE and SSD: Page-Efficient Searchable Symmetric Encryption
Authors: Angèle Bossuat, Raphael Bost, Pierre-Alain Fouque, Brice Minaud, Michael Reichle
Venue: CRYPTO 2021

Abstract: Searchable Symmetric Encryption (SSE) enables a client to outsource a database to an untrusted server, while retaining the ability to securely search the data. The performance bottleneck of classic SSE schemes typically does not come from their fast, symmetric cryptographic operations, but rather from the cost of memory accesses. To address this issue, many works in the literature have considered the notion of locality, a simple design criterion that helps capture the cost of memory accesses in traditional storage media, such as Hard Disk Drives. A common thread among many SSE schemes aiming to improve locality is that they are built on top of new memory allocation schemes, which form the technical core of the constructions.

The starting observation of this work is that for newer storage media such as Solid State Drives (SSDs), which have become increasingly common, locality is not a good

predictor of practical performance. Instead, SSD performance mainly depends on page efficiency, that is, reading as few pages as possible. We define this notion, and identify a simple memory allocation problem, Data-Independent Packing (DIP), that captures the main technical challenge required to build page-efficient SSE. As our main result, we build a page-efficient and storage-efficient data-independent packing scheme, and deduce the Tethys SSE scheme, the first SSE scheme to achieve at once $O(1)$ page efficiency and $O(1)$ storage efficiency. The technical core of the result is a new generalization of cuckoo hashing to items of variable size. Practical experiments show that this new approach achieves excellent performance.

How to (Legally) Keep Secrets from Mobile Operators
Authors: Ghada Arfaoui, Olivier Blazy, Xavier Bultel, Pierre-Alain Fouque, Thibaut Jacques, Adina Nedelcu, Cristina Onete:
Venue: ESORICS 2021

Abstract: Secure-channel establishment allows two endpoints to communicate confidentially and authentically. Since they hide all data sent across them, good or bad, secure channels are often subject to mass surveillance in the name of (inter)national security. Some protocols are constructed to allow easy data interception . Others are designed to preserve data privacy and are either subverted or prohibited to use without trapdoors.

We introduce LIKE, a primitive that provides secure-channel establishment with an exceptional, session-specific opening mechanism. Designed for mobile communications, where an operator forwards messages between the endpoints, it can also be used in other settings. LIKE allows Alice and Bob to establish a secure channel with respect to n authorities. If the authorities all agree on the need for interception, they can ensure that the session key is retrieved. As long as at least one honest authority prohibits interception, the key remains secure; moreover LIKE is versatile with respect to who learns the key. Furthermore, we guarantee non-frameability: nobody can falsely incriminate a user of taking part in a conversation; and honest-operator: if the operator accepts a transcript as valid, then the key retrieved by the authorities is the key that Alice and Bob should compute. Experimental results show that our protocol can be efficiently implemented.

MLS Group Messaging: How Zero-Knowledge Can Secure Updates
Authors: Julien Devigne, Céline Duguey, Pierre-Alain Fouque
Venue: ESORICS 2021

Abstract: The Messaging Layer Security (MLS) protocol currently developed by the Internet Engineering Task Force (IETF) aims at providing a secure group messaging solution. MLS aims for end-to-end security, including Forward Secrecy and Post Compromise Secrecy, properties well studied for one-to-one protocols. It proposes a tree-based regular asynchronous update of the group secrets, where a single user can alone perform a complete update. A main drawback is that a malicious user can create a denial of service attack by sending invalid update information.

In this work, we propose a solution to prevent this kind of attacks, giving a checkpoint role to the server that transmits the messages. In our solution, the user sends to the server a proof that the update has been computed correctly, without revealing any information about this update. We use a Zero-Knowledge (ZK) protocol together with verifiable encryption as building blocks. As a main contribution, we provide two different ZK protocols to prove knowledge of the input of a pseudo random function implemented as a circuit, given an algebraic commitment of the output and the input.

Axis "Malware Analysis"

3.5 Malware Analysis

Participants: Annelie Heuser, Damien Marion, Duy-Phuc Pham.

Collaborations: IRISA, Team DiverSE (Rennes).

Malware analysis is the study or process of determining the functionality, origin and potential impact of a given malware sample such as a virus, worm, trojan horse, rootkit, or backdoor. Malware or malicious software is any computer software intended to harm the host operating system or to steal sensitive data from users, organizations or companies.

At Rennes, we use techniques from side-channel analysis, to detect and identify malware running on embedded devices. We also study packers and similarities of calls dependency graphs.

Accurate and Robust Malware Analysis through Similarity of External Calls Dependency Graphs (ECDG)
Authors: Cassius Puodzius, Olivier Zendra, Annelie Heuser, Lamine Noureddine
Venue: ARES 2021

Abstract: Malware is a primary concern in cybersecurity, being one of the attacker favorite cyberweapons. Over time, malware evolves not only in complexity but also in diversity and quantity. Malware analysis automation is thus crucial. In this paper we present ECDGs, a shorter call graph representation, and a new similarity function that is accurate and robust. Toward this goal, we revisit some principles of malware analysis research to define basic primitives and an evaluation paradigm addressed for the setup of more reliable experiments. Our benchmark shows that our similarity function is very efficient in practice, achieving speedup rates of 3.30x and 354,11x wrt. radiff2 for the standard and the cache-enhanced implementations, respectively. Our evaluations generate clusters that produce almost unerring results - homogeneity score of 0.983 for the accuracy phase - and marginal information loss for a highly polluted dataset -

NMI score of 0.974 between initial and final clusters of the robustness phase. Overall, ECDGs and our similarity function enable autonomous frameworks for malware search and clustering that can assist human-based analysis or improve classification models for malware analysis.

Obfuscation Revealed: Leveraging Electromagnetic Signals for Obfuscated Malware Classification
Authors: Duy-Phuc Pham, Damien Marion, Matthieu Mastio, Annelie Heuser
Venue: ACSAC 2021

Abstract: The Internet of Things (IoT) is constituted of devices that are exponentially growing in number and in complexity. They use numerous customized firmware and hardware, without taking into consideration security issues, which make them a target for cybercriminals, especially malware authors. We will present a novel approach of using side channel information to identify the kinds of threats that are targeting the device. Using our approach, a malware analyst is able to obtain precise knowledge about malware type and identity, even in the presence of obfuscation techniques which may prevent static or symbolic binary analysis. We recorded 100,000 measurement traces from an IoT device infected by various in-the-wild malware samples and realistic benign activity. Our method does not require any modification on the target device. Thus, it can be deployed independently from the resources available without any overhead. Moreover, our approach has the advantage that it can hardly be detected and evaded by the malware authors. In our experiments, we were able to predict three generic malware types (and one benign class) with an accuracy of 99.82%. Even more, our results show that we are able to classify altered malware samples with unseen obfuscation techniques during the training phase, and to determine what kind of obfuscations were applied to the binary, which makes our approach particularly useful for malware analysts.

SE-PAC: A Self-Evolving PAcker Classifier against rapid packers evolution
Authors: Lamine Noureddine, Annelie Heuser, Cassius Puodzius, Olivier Zendra
Venue: CODASPY 2021

Abstract: Packers are widespread tools used by malware authors to hinder static malware detection and analysis. Identifying the packer used to pack a malware is essential to properly unpack and analyze the malware, be it manually or automatically. While many well-known packers are used, there is a growing trend for new custom packers that make malware analysis and detection harder. Research works have been very effective in identifying known packers or their variants, with signature-based, supervised machine learning or similarity-based techniques. However, identifying new packer classes remains an open problem. This paper presents a self-evolving packer classifier that provides an effective, incremental, and robust solution to cope with the rapid evolution of packers. We propose a composite pairwise distance metric combining different types of packer features. We derive an incremental clustering approach able to identify both (variants

of) known packer classes and new ones, as well as to update clusters automatically and efficiently. Our system thus continuously enhances, integrates, adapts and evolves packer knowledge. Moreover, to optimize post clustering packer processing costs, we introduce a new post clustering strategy for selecting small subsets of relevant samples from the clusters. Our approach effectiveness and time-resilience are assessed with: 1) a real-world malware feed dataset composed of 16k packed binaries, comprising 29 unique packers, and 2) a synthetic dataset composed of 19k manually crafted packed binaries, comprising 31 unique packers (including custom ones).

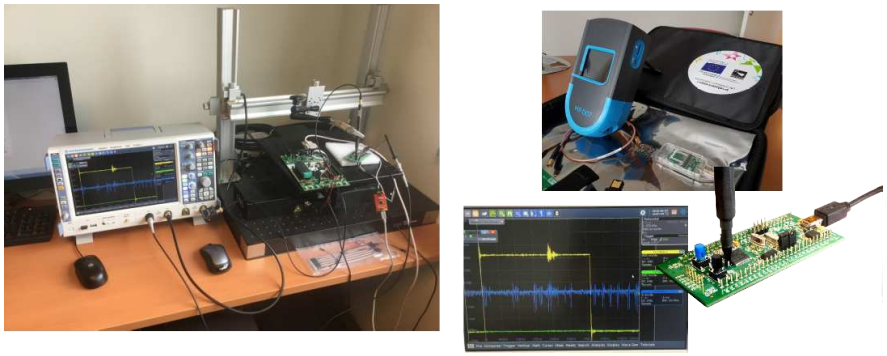
Poster: Obfuscation Revealed - Using Electromagnetic Emanation to Identify and Classify Malware
Authors: Duy-Phuc Pham, Damien Marion, Annelie Heuser
Venue: EuroS&P Workshop 2021

Abstract: In this poster we present a novel approach of using side channel information to identify the kinds of malware threats that are targeting IoT devices. Although in the presence of obfuscation techniques that can prevent static or symbolic binary analysis, a malware researcher may obtain detailed information about malware type and identification using our method by leveraging side channel by electromagnetism rather than software-layer malware analysis. By capturing 100,000 measurement traces from an IoT system infected with different malware samples, we can obtain this information without altering the actual hardware. As a result, it can be implemented without any overhead, regardless of the resources available. Furthermore, our method has the advantage of non-trivial for malware authors to avoid. We were able to distinguish malware families based on side-channel knowledge without being able to see what exact hardware was involved. We were able to predict three generic malware forms (and one benign class) with a 99.89% percent accuracy in our tests. Furthermore, our results show that we are able to classify altered malware samples with unseen obfuscation techniques during the training phase, and to determine what kind of obfuscations, which makes our approach particularly useful for malware analysts.

4 Software development and platforms

4.1 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 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. 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 PROMETHEUS

- Funding: H2020
- Hosting Institution: UR1
- Budget: 520 000 EUR
- PI: Benoît Libert (ENS Lyon)
- CAPSULE: Pierre-Alain and Adeline - UR1 is the leader of Workpackage 4 and Adeline is the Dissemination manager of the project
- Period: 01/01/2018 - 30/06/2022

- URL: `https://www.h2020prometheus.eu/`
- 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 Decrypt

- Funding: ANR
- Hosting Institution: UR1
- Budget CAPSULE:
- PI: Marine Minier (LORIA)
- CAPSULE: Patrick (PI local), 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.

5.2.2 ANR MobiS5

- Funding: ANR
- Hosting Institution: UR1
- Budget total: 637 878 EUR
- Budget CAPSULE: 35 500 EUR
- PI: Cristina Onete (Limoges)

- CAPSULE: Pierre-Alain
- 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.

5.2.3 ANR JCJC CryptAudit

- Funding: ANR
- Hosting Institution: UR1
- Budget: 222 480 EUR
- PI: Patrick Derbez
- CAPSULE: 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-SelÃ§uk Attacks on Block Ciphers; (2) Cryptanalysis of Stream Ciphers; (3) Cryptanalysis of SHA-3; (4) Computer-aided Conception of Symmetric Primitives.

5.2.4 ANR JCJC AHMA

- Funding: ANR
- Hosting Institution: CNRS
- Budget: 342 518,98 EUR
- PI: Annelie Heuser
- CAPSULE: Annelie Heuser, Damien Marion, Duy-Phuc Pham
- Period: 01/04/2019 - 31/03/2022
- URL: `https://anr.fr/Project-ANR-18-CE39-0001`
- Description: The Internet of Things (IoT) will influence the majority of our daily lifeâs infrastructure. While efficiency and diffusion of IoT are increasing, security threats are becoming a far-reaching problem. Here we are particularly concentrating on ensuring the security of IoT nodes against malware threats, which may seriously disrupt daily life and economic activity or even reveal privacy critical data of users. As state-of-the-art software monitoring techniques (static or dynamic) can still be circumvented by sophisticated attackers, we propose an automated hardware malware analysis (AHMA) framework that is non-intrusive and cannot easily be controlled or hidden by the malware attacker. AHMA uses side-channel information of the underlying hardware IoT device to detect if a device is infected by malware (mutated or even unknown) or in its typical running state. Our novel framework is of high importance and impact for industries, and thus for users benefitting from increasing protection.

5.2.5 ANR PCRE IDROMEL

- Funding: ANR
- Hosting Institution: CNRS
- Budget CAPSULE: 170 000 EUR
- local PI: Annelie Heuser

- CAPSULE: Annelie Heuser, Damien Marion, Benoit Gerard, Nicolas Aragon
- Period: 01/01/2021 - 31/12/2025
- Description: SCA typically exploit physical quantities such as power consumption and electromagnetic observations, the observations of the impact of computations on caches, and/or effects due to speculative execution. SCA have gained momentum with the increased use of cryptography because they represent, with fault injection attacks, the most effective way to break cryptographic implementations. For example, the symmetric block cipher AES, which is widely used in most computation systems nowadays because considered secure by the traditional cryptanalysis, is highly vulnerable to side-channel attacks. SCA based on power and electromagnetic observations are particularly harmful for computing objects since they are practical, powerful and hardly detectable. IDROMEL aims at contributing to the design of secure systems against side-channel attacks based on power and electromagnetic observations, for a wide range of computing systems, from cost-effective ones implemented into IoT to more complex architectures commonly integrated into mobile phones.

5.3 Bilateral industry grants

- Grant CIFRE Idemia, Thi-Thu Quyen Nguyen (2021-2024),
- Grant CIFRE Orange Labs, Corentin Jeudy (2021-2024).

5.4 Collaborations

5.4.1 Visited Labs

- Alexandre Wallet visited the LFANT team in Institut Mathématiques de Bordeaux (IMB) from 8th to 11th November 2021.

6 Dissemination

6.1 Promoting scientific activities

- Pierre-Alain Fouque is a member of the *Institut Universitaire de France*. He is also Responsible for the Master Cybersécurité at Rennes 1 University. He was the PI for the ANR SafeTLS projects and works in the Prometheus European Project. He was a member of the evaluation committee for the European Research Council. 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. He was responsible for the PEPR project in Post-Quantum Cryptography with a funding of 8,5 Meuros. He is also a member of the committee of EPIT and in the Steering committee of CHES.

- 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.
- Annelie Heuser is the PI of the JCJC ANR AHMA project and the local PI of the ANR PRCE IDROMEL project. She was a PC member of Eurocrypt, TCHES, COSADE, DATE, VLSID Design conferences.
- Adeline Roux-Langlois is co-responsible of the Cryptography Seminar (DGA, IRMAR, IRISA) in Rennes. She was Dissemination manager of the H2020 Project Prometheus. She is also member of the scientific committee of the C2 seminar (organised by the GT-C2) which is in Paris (4 times a year). She was a PC member of the Eurocrypt and Indocrypt conferences.
- Alexandre Wallet is a member of the organizing committee of the Cryptography Seminar (DGA, IRMAR, IRISA) in Rennes. He was a PC member of the ANTS conference.

6.2 Teaching and Juries

6.2.1 Teaching

- Patrick Derbez is in charge of a 48-hour course “Algorithms for Security” (4th-year students), of a 12-hour course “Symmetric cryptography” (5th-year students), and the imperative course for first-year student at the University of Rennes.
- Pierre-Alain Fouque is in charge of a 32-hour course “Cryptography” (5th-year students), of a 48-hour course “Introduction to Security” (4th-year students), and of a 32-hour “Algorithms" course at Rennes University. He also teaches in an introductory course of imperative programming in Java for all first-year students in the Maths and CS departments of the Rennes 1 University.
- Adeline Roux-Langlois is in charge of a 24-hour course on “Introduction to Cryptography” (1st year students at ENS Rennes), and of a 20-hours course on "Algorithmic" (M1 MEEF), and co-lecture 24 hours in a 32h course “Lattices for cryptography” (5th year students, UR1).
- Alexandre Wallet is Assistant Professor at École Polytechnique for 64 hours, shared between “Advanced Programming” for first-year bachelor students and “Introduction to Programming” for third-year engineer students. He was also responsible of 12 hours in “Lattices for cryptography” (5th year students, UR1).

6.2.2 PhD and HDR Juries

- EMSEC PHD defences
  - Katharina Boudgoust, UR1, November 2021 (Adeline Roux-Langlois and Pierre-Alain Fouque was “co-Director’),
  - Céline Duguey, UR1, December 2021 (Pierre-Alain Fouque was “Directeur’),
  - Victor Mollimard, UR1, January 2022 (Pierre-Alain Fouque was “Directeur’, and Patrick Derbez was "supervisor"),
  - Adina Nedelcu, UR1, January 2022 (Pierre-Alain Fouque was “Director”).

- PHD defences
  - Daniel Coggia, Sorbonnes University, October 2021 (Pierre-Alain Fouque was "Reviewer")
  - Huyen Nguyen, ENS Lyon, November 2021 (Adeline Roux-Langlois was "Reviewer")
  - Rémi Clarisse, UR1, December 2021 (Pierre-Alain Fouque was “Examinateur”)
  - Kuo Zhao, Monash University, December 2021 (Pierre-Alain Fouque was “Reviewer”)
  - Natalia Kulatova, ENS, January 2022 (Pierre-Alain Fouque was “Reviewer and President”)
  - Kostas Papagiannopoulis, Radboud University, 2021 (Annelie Heuser was “Reviewer”)
  - Loic Masure CEA, 2021, (Annelie Heuser was “Reviewer”)
  - Wei Chung, Telecom ParisTech, 2021 (Annelie Heuser was “Reviewer”)

6.3 Popularization

- Patrick’s work on GEA attacks received a worldwide audience such as `https://www.schneier.com/blog/archives/2021/06/intentional-flaw-in-gprs-encryption-algorithm-gea-1.html`
- Adeline Roux-Langlois was interviewed in CNRS le journal, article "Vers une cryptographie post-quantique" from Martin Koppe. https://lejournal.cnrs.fr/articles/vers-une-cryptographie-post-quantique, April 2021.
- several articles have been published about the paper ”Obfuscation Revealed: Leveraging Electromagnetic Signals for Obfuscated Malware Classification” published at ACSAC 2021, e.g.:
  - Using EM Waves to Detect Malware. Schneier on security. January 15, schneier. (n.d.). Retrieved January 21, 2022, from `https://www.schneier.com/blog/archives/2022/01/using-em-waves-to-detect-malware.html`
  - Computer Sweden. Accessed 21 January 2022. `https://computersweden.idg.se/2.2683/1.761341/skadlig-kod-kan-upptackas-med-elektromagnetiska-vagor`.
  - Identifying Malware By Sniffing Its EM Signature. Tom Nardi. Hackaday (blog), 19 January 2022. `https://hackaday.com/2022/01/19/identifying-malware-by-sniffing-its-em-signature/`.
  - Tracy, P. (2022, January 12). Raspberry pi can detect malware by scanning for electromagnetic waves. Gizmodo. Retrieved January 21, 2022, from `https://gizmodo.com/raspberry-pi-can-detect-malware-by-scanning-for-electro-1848339130`

– Detecting evasive malware on IOT devices using electromagnetic emanations. The Hacker News. (2022, January 6). Retrieved January 11, 2022, from https://thehackernews.com/2022/01/detecting-evasive-malware-on-iot.html

– Matthew is PCMag's UK-based editor and news reporter. Prior to joining the team. (2022, January 10). No software required: Raspberry Pi uses electromagnetic waves to detect malware. PCMag UK. Retrieved January 11, 2022, from https://uk.pcmag.com/malware-protection-removal/138056/no-software-required-raspberry-pi-uses-electromagnetic-waves-to-detect-malware (2022, January 11).

– Raspberry pi peut desormais Detecter Les malwares sans logiciel. hitechglitz.com. Retrieved January 11, 2022, from https://hitechglitz.com/france/raspberry-pi-peut-desormais-detecter-les-malwares-sans-logiciel/

– Hill, A. (2022, January 9). Raspberry pi detects malware using electromagnetic waves. Tom's Hardware. Retrieved January 11, 2022, from https://www.tomshardware.com/news/raspberry-pi-detects-malware-with-em-waves (2022, January 11).

Articles in referred journals and book chapters

[1] L. Batina, M. Djukanovic, A. Heuser, S. Picek, "It Started with Templates: The Future of Profiling in Side-Channel Analysis", *in : Security of Ubiquitous Computing Systems*, 2021, p. 133 – 145, https://hal.inria.fr/hal-03458797.

[2] T. Trouchkine, S. K. K. Bukasa, M. Escouteloup, R. Lashermes, G. Bouffard, "Electromagnetic fault injection against a complex CPU, toward new micro-architectural fault models", *Journal of Cryptographic Engineering 11*, 4, November 2021, p. 353–367, https://hal.archives-ouvertes.fr/hal-03175704.

Publications in Conferences and Workshops

[3] G. ARFAOUI, O. Blazy, X. Bultel, P.-A. Fouque, T. Jacques, A. Nedelcu, C. Onete, "How to (Legally) Keep Secrets from Mobile Operators", *in : Computer Security - ESORICS 2021 - 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4-8, 2021, Proceedings, Part I*, E. Bertino, H. Shulman, M. Waidner (editors), *Lecture Notes in Computer Science*, *12972*, Springer, p. 23–43, Online, Unknown Region, 2021, https://hal-polytechnique.archives-ouvertes.fr/hal-03478246.

[4] C. Beierle, P. Derbez, G. Leander, G. Leurent, H. Raddum, Y. Rotella, D. Rupprecht, L. Stennes, "Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2", *in : EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, *Lecture Notes in Computer Science*, *12697*, Springer, p. 155–183, Zagreb, Croatia, October 2021, https://hal.inria.fr/hal-03529373.

[5] P. Bert, G. Eberhart, L. Prabel, A. Roux-Langlois, M. Sabt, "Implementation of Lattice Trapdoors on Modules and Applications", *in : PQCrypto 2021 - International*

Conference on Post-Quantum Cryptography, *Lecture Notes in Computer Science*, 12841, p. 195 – 214, Virtual event, France, July 2021, https://hal.archives-ouvertes.fr/hal-03355923.

[6] A. Bossuat, R. Bost, P.-A. Fouque, B. Minaud, M. Reichle, "SSE and SSD: Page-Efficient Searchable Symmetric Encryption", *in : Crypto 2021 - Annual International Cryptology Conference*, Virtual, France, August 2021, https://hal.inria.fr/hal-03377462.

[7] K. Boudgoust, C. Jeudy, A. Roux-Langlois, W. Wen, "On the Hardness of Module-LWE with Binary Secret", *in : Topics in Cryptology – CT-RSA 2021*, K. G. Paterson (editor), *Topics in Cryptology – CT-RSA 2021*, *12704*, Cryptographers' Track at the RSA Conference 2021, Springer, p. 503–526, San Francisco, United States, May 2021, https://hal.archives-ouvertes.fr/hal-03264223.

[8] D. De Almeida Braga, P.-A. Fouque, M. Sabt, "PARASITE: PAssword Recovery Attack against Srp Implementations in ThE wild", *in : CCS 2021 - ACM SIGSAC Conference on Computer and Communications Security*, *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, ACM, p. 2497–2512, Virtual Event, South Korea, November 2021, https://hal.archives-ouvertes.fr/hal-03551345.

[9] S. Delaune, P. Derbez, A. Gontier, C. Prud'Homme, "A Simpler Model for Recovering Superpoly on Trivium", *in : Selected Areas in Cryptography SAC 2021*, Victoria, British-Columbia, Canada, September 2021, https://hal.archives-ouvertes.fr/hal-03534492.

[10] S. Delaune, P. Derbez, P. Huynh, M. Minier, V. Mollimard, C. Prud'Homme, "Efficient Methods to Search for Best Differential Characteristics on SKINNY", *in : ACNS 2021 - 19th International Conference on Applied Cryptography and Network Security*, K. Sako, N. O. Tippenhauer (editors), *19th International Conference on Applied Cryptography and Network Security*, *12727*, p. 184–207, Kamakura, Japan, June 2021, https://hal.archives-ouvertes.fr/hal-03040548.

[11] J. Devigne, C. Duguey, P. Fouque, "MLS Group Messaging: How Zero-Knowledge Can Secure Updates", *in : Computer Security - ESORICS 2021 - 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4-8, 2021, Proceedings, Part II*, E. Bertino, H. Shulman, M. Waidner (editors), *Lecture Notes in Computer Science*, *12973*, Springer, p. 587–607, 2021, https://doi.org/10.1007/978-3-030-88428-4_29.

[12] M. Escouteloup, R. Lashermes, J. Fournier, J.-L. Lanet, "Under the dome: preventing hardware timing information leakage", *in : CARDIS 2021 - 20th Smart Card Research and Advanced Application Conference*, *CARDIS: International Conference on Smart Card Research and Advanced Applications*, p. 1–20, Lübeck, Germany, November 2021, https://hal.archives-ouvertes.fr/hal-03351957.

[13] C. Genevey-Metat, A. Heuser, G. Benoit, "Train or Adapt a Deeply Learned Profile?", *in : LATINCRYPT 2021 - 7th International Conference on Cryptology and Information Security in Latin America*, Bogota, Colombia, October 2021, https://hal.inria.fr/hal-03458681.

[14] C. Genevey-Metat, A. Heuser, B. Gérard, "Trace-to-trace translation for SCA", *in : CARDIS 2021 - 20th Smart Card Research and Advanced Application Conference*, Luebeck, Germany, November 2021, https://hal.inria.fr/hal-03553723.

[15] G. Kaim, S. Canard, A. Roux-Langlois, J. Traoré, "Post-quantum Online Voting Scheme", *in : FC 2021 - Financial Cryptography and Data Security. International Workshops*, *Lecture Notes in Computer Science*, 12676, p. 290–305, Virtual event, France, March 2021, https://hal.archives-ouvertes.fr/hal-03355875.

[16] P. Kirchner, T. Espitau, P. Fouque, "Towards Faster Polynomial-Time Lattice Reduction", *in : Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part II*, T. Malkin, C. Peikert (editors), *Lecture Notes in Computer Science*, *12826*, Springer, p. 760–790, 2021, https://doi.org/10.1007/978-3-030-84245-1_26.

[17] L. Noureddine, A. Heuser, C. Puodzius, O. Zendra, "SE-PAC: A Self-Evolving PAcker Classifier against rapid packers evolution", *in : CODASPY '21 - 11th ACM Conference on Data and Application Security and Privacy*, ACM, p. 1–12, Virtual Event, United States, April 2021, https://hal.inria.fr/hal-03149211.

[18] D.-P. Pham, D. Marion, M. Mastio, A. Heuser, "Obfuscation Revealed: Leveraging Electromagnetic Signals for Obfuscated Malware Classification", *in : ACSAC 2021 - Annual Computer Security Applications Conference*, ACM, p. 1–14, Virtual Event, France, December 2021, https://hal.archives-ouvertes.fr/hal-03374399.

[19] C. Puodzius, O. Zendra, A. Heuser, L. Noureddine, "Accurate and Robust Malware Analysis through Similarity of External Calls Dependency Graphs (ECDG)", *in : ARES 2021 - The 16th International Conference on Availability, Reliability and Security*, ACM, p. 1–12, Virtual, Austria, August 2021. This paper received the Best Paper Award for IWCC 2021, https://hal.archives-ouvertes.fr/hal-03328395.

Miscellaneous

[20] A. Heuser, D.-P. Pham, D. Marion, A. Heuser, "Poster: Obfuscation Revealed - Using Electromagnetic Emanation to Identify and Classify Malware", EuroS
P 2021 - 6th IEEE European Symposium on Security and Privacy, September 2021, Poster, https://hal.inria.fr/hal-03458819.