

Clémentine MAURICE

Chargée de Recherche CNRS

Inria, Parc scientifique de la Haute-Borne
40 Avenue Halley, Bâtiment B
59650 Villeneuve-d'Ascq
✉ clementine.maurice@cnrs.fr
🌐 cmaurice.fr
1 enfant né 09/2023

Thématiques de recherche

Mes travaux et mon projet de recherche portent sur la **sécurité** et la protection de la vie privée, du point de vue des systèmes d'information, et plus précisément dans l'**interaction entre le logiciel et le matériel**. Mes travaux de recherche s'attachent à analyser les fuites d'informations sensibles dues à la **micro-architecture des processeurs** et les attaques par fautes ne requérant aucun accès matériel. Ma recherche a pour but de créer des contre-mesures à ces attaques qui soient à la fois robustes, performantes, et adaptées aux appareils du quotidien tels que les appareils mobiles, les ordinateurs portables et personnels ainsi que les serveurs dans les environnements de type cloud computing. Une première étape nécessaire est la recherche des vecteurs d'attaques ainsi que l'évaluation du réalisme de ces attaques. Ces attaques exploitant des composants très complexes et souvent non documentés, un de mes axes de recherche consiste également en la rétro-ingénierie de ces composants matériels.

Curriculum Vitae

depuis 2021 **Chargée de Recherche CNRS**, équipe *Spirals*, *CRISAL*, Lille.

HDR : "Micro-architectural side channels: Studying the attack surface from hardware to browsers".
Soutenue le 24 mai 2023 à l'Université de Lille.

Jury : Davide Balzarotti, Lejla Batina, Tamara Rezk, Herbert Bos, Gilles Grimaud, Romain Rouvoy.

- Interruption de carrière : Congé maternité d'août 2023 à février 2024 (6 mois).

2017–2021 **Chargée de Recherche CNRS**, équipe *EMSEC*, *IRISA*, Rennes.

2016–2017 **Chercheuse postdoctorale**, équipe *Secure Systems*, *IAIK*, *TU Graz*, Autriche.

2012–2015 **Doctorante**, *CIFRE Eurecom/Technicolor*, Sophia Antipolis et Cesson-Sévigné.

Thèse de doctorat : "Fuites d'information dans les processeurs récents et applications à la virtualisation".
Soutenue le 28 octobre 2015 à Télécom ParisTech.

Directeurs de thèse : Aurélien Francillon et Christoph Neumann. Encadrant : Olivier Heen.

- Visite de deux semaines dans l'équipe *Secure Systems* de *TU Graz* en Autriche pour travailler sur la première attaque par faute logicielle depuis un navigateur en JavaScript [23].

Publications

Les conférences reconnues par les pairs comme étant les meilleures dans le domaine de la sécurité informatique sont ACM CCS, IEEE S&P, Usenix Security et NDSS. Le taux d'acceptation est donné pour chaque conférence, quand il est connu. Dans mon domaine, il est d'usage que les auteurs soient ordonnés par rapport à leurs contributions respectives. Ma visibilité est reflétée par mon h-index de 21 ainsi que mes 5303 citations (selon Google Scholar en mars 2024).

Revue internationale avec comité de lecture

- [1] Michael Schwarz, Samuel Weiser, Daniel Gruss, Clémentine Maurice, and Stefan Mangard. "Malware Guard Extension: Abusing Intel SGX to conceal cache attacks". In: *Cybersecurity* 3 (Jan. 2020).
- [2] Sarani Bhattacharya, Clémentine Maurice, Shivam Bhasin, and Debdeep Mukhopadhyay. "Branch Prediction Attack on Blinded Scalar Multiplication". In: *IEEE Transactions on Computers* 69.5 (2020), pp. 633–648.

Conférences internationales avec comité de lecture

- [3] Antoine Geimer, Mathéo Vergnolle, Frédéric Recoules, Lesly-Ann Daniel, Sébastien Bardin, and Clémentine Maurice. "A Systematic Evaluation of Automated Tools for Side-Channel Vulnerabilities Detection in Cryptographic Libraries". In: *Proceedings of the 2023 Conference on Computer and Communications Security*. CCS. Taux d'acceptation : 19.1%. ACM, Nov. 2023.
- [4] Marina Botvinnik, Tomer Laor, Thomas Rokicki, Clémentine Maurice, and Yossi Oren. "The Finger in the Power: How to Fingerprint PCs by Monitoring Their Power Consumption". In: *Proceedings of the 20th Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. DIMVA. Taux d'acceptation : 28.3%. Springer, July 2023.

- [5] Guillaume Didier, Clémentine Maurice, Antoine Geimer, and Walid Ghandour. "Characterizing Prefetchers using CacheObserver". In: *Proceedings of the 34th International Symposium on Computer Architecture and High Performance Computing*. SBAC-PAD. IEEE, Nov. 2022.
- [6] Thomas Rokicki, Clémentine Maurice, and Michael Schwarz. "CPU Port Contention Without SMT". In: *Proceedings of the 27th European Symposium on Research in Computer Security*. ESORICS. Taux d'acceptation : 18.5%. Springer, Sept. 2022.
- [7] Thomas Rokicki, Clémentine Maurice, Marina Botvinnik, and Yossi Oren. "Port Contention Goes Portable: Port Contention Side Channels in Web Browsers". In: *Proceedings of the 17th ACM ASIA Conference on Computer and Communications Security*. ASIACCS. Taux d'acceptation : 18.4%. ACM, May 2022, pp. 1182–1194.
- [8] Tomer Laor, Naif Mehanna, Antonin Durey, Vitaly Dyadyuk, Pierre Laperdrix, Clémentine Maurice, Romain Rouvoy Yossi Oren, Walter Rudametkin, and Yuval Yarom. "DrawnApart: A Device Identification Technique based on Remote GPU Fingerprinting". In: *Proceedings of the Annual Network and Distributed System Security Symposium*. NDSS. Taux d'acceptation : 16.2%. The Internet Society, Apr. 2022.
- [9] Thomas Rokicki, Clémentine Maurice, and Pierre Laperdrix. "SoK: In Search of Lost Time: A Review of JavaScript's Timers in Browsers". In: *Proceedings of the 6th IEEE European Symposium on Security and Privacy*. EuroS&P. Taux d'acceptation : 19.4%. IEEE, Sept. 2021.
- [10] Guillaume Didier and Clémentine Maurice. "Calibration Done Right: Noiseless Flush+Flush Attacks". In: *Proceedings of the 18th Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. DIMVA. Taux d'acceptation : 28.8%. Springer, July 2021.
- [11] Moritz Lipp, Vedad Hadžić, Michael Schwarz, Arthur Perais, Clémentine Maurice, and Daniel Gruss. "Take A Way: Exploring the Security Implications of AMD's Cache Way Predictors". In: *Proceedings of the 15th ACM ASIA Conference on Computer and Communications Security*. ASIACCS. Taux d'acceptation : 21.8%. ACM, June 2020.
- [12] Michael Schwarz, Daniel Gruss, Moritz Lipp, Clémentine Maurice, Thomas Schuster, Anders Fogh, and Stefan Mangard. "Automated Detection, Exploitation, and Elimination of Double-Fetch Bugs using Modern CPU Features". In: *Proceedings of the 13th ACM Asia Conference on Computer and Communications Security*. ASIACCS. Taux d'acceptation : 20.0%. ACM, May 2018.
- [13] Michael Schwarz, Moritz Lipp, Daniel Gruss, Samuel Weiser, Clémentine Maurice, Raphael Spreitzer, and Stefan Mangard. "KeyDrown: Eliminating Software-Based Keystroke Timing Side-Channel Attacks". In: *Proceedings of the 25th Annual Network and Distributed System Security Symposium*. NDSS. Taux d'acceptation : 21.5%. The Internet Society, Feb. 2018.
- [14] Moritz Lipp, Daniel Gruss, Michael Schwarz, David Bidner, Clémentine Maurice, and Stefan Mangard. "Practical Keystroke Timing Attacks in Sandboxed JavaScript". In: *Proceedings of the 22nd European Symposium on Research in Computer Security*. ESORICS. Taux d'acceptation : 15.9%. Springer, Sept. 2017.
- [15] Daniel Gruss, Moritz Lipp, Michael Schwarz, Richard Fellner, Clémentine Maurice, and Stefan Mangard. "KASLR is Dead: Long Live KASLR". In: *Proceedings of the 9th International Symposium on Engineering Secure Software and Systems*. ESSoS. Taux d'acceptation : 46.9%. Springer, July 2017.
- [16] Michael Schwarz, Samuel Weiser, Daniel Gruss, Clémentine Maurice, and Stefan Mangard. "Malware Guard Extension: Using SGX to Conceal Cache Attacks". In: *Proceedings of the 14th Conference on Detection of Intrusions and Malware & Vulnerability Assessment*. DIMVA. Taux d'acceptation : 26.9%. Springer, July 2017.
- [17] Michael Schwarz, Clémentine Maurice, Daniel Gruss, and Stefan Mangard. "Fantastic Timers and Where to Find Them: High-Resolution Microarchitectural Attacks in JavaScript". In: *Proceedings of the 21st International Conference on Financial Cryptography and Data Security*. FC. Springer, Apr. 2017.
- [18] Clémentine Maurice, Manuel Weber, Michael Schwarz, Lukas Giner, Daniel Gruss, Carlo Alberto Boano, Stefan Mangard, and Kay Römer. "Hello from the Other Side: SSH over Robust Cache Covert Channels in the Cloud". In: *Proceedings of the 24th Annual Network and Distributed System Security Symposium*. NDSS. Taux d'acceptation : 16.1%. The Internet Society, Feb. 2017.
- [19] Daniel Gruss, Clémentine Maurice, Anders Fogh, Moritz Lipp, and Stefan Mangard. "Prefetch Side-Channel Attacks: Bypassing SMAP and Kernel ASLR". In: *Proceedings of the 23rd ACM Conference on Computer and Communications Security*. CCS. Taux d'acceptation : 16.4%. ACM, Nov. 2016.
- [20] Victor van der Veen, Yanick Fratantonio, Martina Lindorfer, Daniel Gruss, Clémentine Maurice, Giovanni Vigna, Herbert Bos, Kaveh Razavi, and Cristiano Giuffrida. "Drammer: Deterministic Rowhammer Attacks on Mobile Platforms". In: *Proceedings of the 23rd ACM Conference on Computer and Communications Security*. CCS. Taux d'acceptation : 16.4%. ACM, Nov. 2016.

- [21] Moritz Lipp, Daniel Gruss, Raphael Spreitzer, Clémentine Maurice, and Stefan Mangard. “ARMageddon: Cache Attacks on Mobile Devices”. In: *Proceedings of the 25th USENIX Security Symposium*. USENIX Security. Taux d’acceptation : 15.6%. USENIX Association, Aug. 2016, pp. 549–564.
- [22] Peter Pessl, Daniel Gruss, Clémentine Maurice, Michael Schwarz, and Stefan Mangard. “DRAMA: Exploiting DRAM Addressing for Cross-CPU Attacks”. In: *Proceedings of the 25th USENIX Security Symposium*. USENIX Security. Taux d’acceptation : 15.6%. USENIX Association, Aug. 2016, pp. 565–581.
- [23] Daniel Gruss, Clémentine Maurice, and Stefan Mangard. “Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript”. In: *Proceedings of the 13th Conference on Detection of Intrusions and Malware & Vulnerability Assessment*. DIMVA. Taux d’acceptation : 31.8%. Springer, July 2016, pp. 300–321.
- [24] Daniel Gruss, Clémentine Maurice, Klaus Wagner, and Stefan Mangard. “Flush+Flush: A Fast and Stealthy Cache Attack”. In: *Proceedings of the 13th Conference on Detection of Intrusions and Malware & Vulnerability Assessment*. DIMVA. Taux d’acceptation : 31.8%. Springer, July 2016, pp. 279–299.
- [25] Clémentine Maurice, Nicolas Le Scouarnec, Christoph Neumann, Olivier Heen, and Aurélien Francillon. “Reverse Engineering Intel Last-Level Cache Complex Addressing Using Performance Counters”. In: *Proceedings of the 18th International Symposium on Research in Attacks, Intrusions and Defenses*. RAID. Taux d’acceptation : 23.5%. Springer, Nov. 2015, pp. 48–65.
- [26] Clémentine Maurice, Christoph Neumann, Olivier Heen, and Aurélien Francillon. “C5: Cross-Cores Cache Covert Channel”. In: *Proceedings of the 12th Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. DIMVA. Taux d’acceptation : 22.7%. Springer, July 2015, pp. 46–64.
- [27] Clémentine Maurice, Christoph Neumann, Olivier Heen, and Aurélien Francillon. “Confidentiality Issues on a GPU in a Virtualized Environment”. In: *Proceedings of the 18th International Conference on Financial Cryptography and Data Security*. FC. Taux d’acceptation : 22.5%. Springer, Mar. 2014, pp. 119–135.
- [28] Clémentine Maurice, Stéphane Onno, Christoph Neumann, Olivier Heen, and Aurélien Francillon. “Improving 802.11 Fingerprinting of Similar Devices by Cooperative Fingerprinting”. In: *Proceedings of the 2013 International Conference on Security and Cryptography*. SECRIPT. Springer, Aug. 2013, pp. 379–386.

Workshops internationaux avec comité de lecture

- [29] Walid Ghandour and Clémentine Maurice. “DITTANY: Strength-Based Dynamic Information Flow Analysis Tool for x86 Binaries”. In: *Binary Analysis Research Workshop (BAR)*. co-localisé avec NDSS. Apr. 2022.
- [30] Quentin Forcioli, Jean-Luc Danger, Clémentine Maurice, Lilian Bossuet, Florent Bruguier, Maria Mushtaq, David Novo, Loïc France, Pascal Benoit, Sylvain Guilley, and Thomas Perianin. “Virtual Platform to Analyze the Security of a System on Chip at Microarchitectural Level”. In: *Proceedings of the 2021 Workshop on the Security of Software / Hardware Interfaces (SILM)*. co-localisé avec EuroS&P. Sept. 2021.
- [31] Pierre Ayoub and Clémentine Maurice. “Reproducing Spectre Attack with gem5: How To Do It Right?”. In: *Proceedings of the 14th European Workshop on Systems Security*. EuroSec. co-localisé avec EuroSys. ACM, Apr. 2021.
- [32] Moritz Lipp, Misiker Tadesse Aga, Michael Schwarz, Daniel Gruss, Clémentine Maurice, Lukas Raab, and Lukas Lamster. “Nethammer: Inducing Rowhammer Faults through Network Requests”. In: *Proceedings of the 2020 Workshop on the Security of Software / Hardware Interfaces (SILM)*. co-localisé avec EuroS&P. June 2020.

Articles de vulgarisation

- [33] Clémentine Maurice. “Meltdown et attaques sur KASLR : les attaques par canal auxiliaire passent à la vitesse supérieure”. In: *MISC n°97* (May 2018).
- [34] Clémentine Maurice. “Après Meltdown et Spectre, comment sécuriser les processeurs ?” In: *Le Journal du CNRS* (Mar. 2018).

Brevets

- [35] Clémentine Maurice, Olivier Heen, Christoph Neumann, and Aurélien Francillon. *Method and apparatus for cross-core covert channel*. US Patent 20,160,117,246. Apr. 2016.
- [36] Christoph Neumann, Olivier Heen, and Clémentine Maurice. *Device and method for record linkage*. European Patent Application EP 3 093 776 A1. Nov. 2016.
- [37] Christoph Neumann, Olivier Heen, Clémentine Maurice, and Stéphane Onno. *Method and device for countering fingerprint forgery attacks in a communication system*. US Patent 9,143,528. Sept. 2015.

Service académique et responsabilités administratives

- Membre du Collège Codes sources et logiciels du Comité pour la Science Ouverte du MESR depuis 2022

Membre de comités de pilotage de conférences et de workshops

- Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) depuis 2021
- Workshop on Offensive Technologies (WOOT) depuis 2020

Responsable de comités de programme de conférences et de workshops — le classement Core est donné quand il est connu (<http://portal.core.edu.au/conf-ranks>)

- USENIX Security Symposium 2022, rang A*, **Artifact Evaluation Committee co-chair**
- USENIX Security Symposium 2021, rang A*, **Artifact Evaluation Committee co-chair**
- Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) 2020, rang C, **PC chair**
- Workshop on Offensive Technologies (WOOT) 2019 (co-localisé avec Usenix Security), **PC co-chair, Artifact Evaluation Committee co-chair**
- Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) 2019, rang C, **PC co-chair**

Membre de comités de programme de conférences internationales — le classement Core est donné quand il est connu (<http://portal.core.edu.au/conf-ranks>)

- International Symposium on Research in Attacks, Intrusions and Defenses (**RAID**) 2024, rang A
- ACM Conference on Computer and Communications Security (**CCS**) 2022, rang A*
- IEEE Symposium on Security and Privacy (**S&P**) 2022, rang A*
- USENIX Security Symposium (**USENIX Sec**) 2021, rang A*
- IEEE Symposium on Security and Privacy (**S&P**) 2021, rang A*
- USENIX Security Symposium (**USENIX Sec**) 2020, rang A*
- IEEE Symposium on Security and Privacy (**S&P**) 2020, rang A*
- Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) 2018, rang C
- International Conference on Distributed Computing Systems (**ICDCS**) 2018, Security track, rang A
- World Wide Web Conference (**WWW**) 2018, Security and Privacy research track, rang A*
- Conference on Cryptographic Hardware and Embedded Systems (**CHES**) 2018, rang A
- Annual Computer Security Applications Conference (**ACSAC**) 2017, rang A
- International Symposium on Engineering Secure Software and Systems (ESSoS) 2017

Membre de comités de programme de workshops internationaux et de conférences nationales

- Workshop on the Security of Software/Hardware Interfaces (SILM) 2023 (co-localisé avec EuroS&P)
- Workshop on Offensive Technologies (WOOT) 2023 (co-localisé avec S&P)
- Symposium sur la sécurité des technologies de l'information et des communications (SSTIC) 2022
- Hardware and Architectural Support for Security and Privacy (HASP) 2021 (co-localisé avec MICRO)
- First Workshop on DRAM Security (DRAMSec) 2021 (co-localisé avec ISCA)
- Symposium sur la sécurité des technologies de l'information et des communications (SSTIC) 2020
- Symposium sur la sécurité des technologies de l'information et des communications (SSTIC) 2019
- European Workshop on Systems Security (EuroSec) 2019
- Reversing and Offensive-oriented Trends Symposium (ROOTS) 2018
- Workshop on Offensive Technologies (WOOT) 2018 (co-localisé avec USENIX Security)
- Symposium sur la sécurité des technologies de l'information et des communications (SSTIC) 2018

Relectrice pour des revues internationales à comité de lecture

- IEEE Transactions on Information Forensics & Security (T-IFS), 2022, 2014
- Journal of Computer Security, 2019
- ACM Transactions on Embedded Computing Systems, 2019
- IEEE Transactions on Emerging Topics in Computing (TETC), 2017
- Elsevier Microprocessors and Microsystems (MICPRO), 2017
- ACM Transactions on Internet Technology (TOIT), 2016

Relectrice externe : SAC 2019, CCS 2017, VLSI-SoC 2017, DIMVA 2017, RAID 2017, AsiaCCS 2017, DATE 2017, NDSS 2017, ACSAC 2016, ICDCS 2016, WOOT 2015, Eurosec 2013, ESORICS 2013

Membre de comités de sélection et de prix

- Membre de comité de sélection de Maître de Conférences à l'Université Grenoble Alpes, 2023
- Membre de comité de sélection de Maître de Conférences à l'Université de Rennes 1, 2022
- Membre de comité de sélection de Maître de Conférences à l'ENS de Rennes, 2021
- Membre de comité de sélection de Maître de Conférences à l'Université de Lorraine, 2021
- Secrétaire du prix de thèse Gilles Kahn de la Société Informatique de France (SIF), 2019, 2020, 2021

- Membre du jury de prix de thèse Gilles Kahn de la Société Informatique de France (SIF), 2018
- Membre de comité de sélection de Maître de Conférences à l'INSA de Toulouse, 2018

Responsabilités administratives

- Co-animatrice de l'axe transversal "Cybersécurité" du laboratoire CRISStAL, depuis 2023
- Membre de la cellule "Parité-égalité" du laboratoire CRISStAL, depuis 2021
 - Co-responsable de la création et de l'animation du programme de mentorat au laboratoire, depuis 2021
 - Co-organisation de réunions d'échanges mixtes autour de la parité ("100% parité"), depuis 2023
 - Création d'affichettes de sensibilisation aux violences sexistes et sexuelles pour le laboratoire, 2023
 - Co-organisation de déjeuners entre femmes ("Girls Only"), 2022-2023
- Membre de la commission électorale du conseil de laboratoire de l'IRISA, 2018

Expertise

- Evaluation de projet pour Israel Science Foundation (ISF), 2022

Jurys de thèses (14)

France (x9), Pays-Bas (x2), Espagne (x1), Finlande (x1), Italie (x1).

- Pietro Borello, "Taming Complex Bugs in Secure Systems", Sapienza Università di Roma, Italie, Mai 2023 (external reviewer)
- Amine Jaamoum, "Stratégies de sécurisation d'une hiérarchie mémoire contre les attaques par canaux auxiliaires logiciels" Université Grenoble Alpes, France, Décembre 2022
- Hadrien Barral, "Embedded devices security: shellcoding, forensics and operating systems", ENS Paris, France, Septembre 2022
- Ben Gras, "Information Security Risks of Commodity Architectures in Shared Computing Environments", VU Amsterdam, Pays-Bas, Juin 2022
- Cesar Pereida García, "Side-Channel Analysis and Cryptography Engineering", Tampere University, Finlande, Février 2022 (dissertation pre-examiner)
- Mathieu Escouteloup, "Micro-architectures Sécurisées", Université de Rennes 1, France, Décembre 2021
- Georges-Axel Jaloyan, "A Semantic Approach to Machine-Level Software Security", ENS Paris, France, Septembre 2021
- Thomas Troughkine, "Evaluation de la sécurité Physique des SoC", Université Grenoble Alpes, France, Mars 2021
- Nampoina Andriamilanto, "Leveraging Browser Fingerprinting for Web Authentication", Université de Rennes 1, France, Décembre 2020
- Sébastien Carré, "Attaques exploitant le temps de calcul : modélisation et protections", Télécom Paris, France, Décembre 2020
- Radhesh Konoth, "Vulnerable by Design: Mitigating Design Flaws in Hardware and Software", VU Amsterdam, Pays-Bas, Décembre 2020
- Pepe Vila, "Learning Secrets and Models from Execution Time", IMDEA Software Institute, Espagne, Juin 2020
- Antoine Vastel, "Tracking Versus Security: Investigating the Two Facets of Browser Fingerprinting", Université de Lille, France, Octobre 2019
- Fabio Pagani, "Advances in memory forensics", EURECOM, France, Septembre 2019

Organisation d'événements

- Co-organisation d'un séminaire Dagstuhl "MAD: Microarchitectural Attacks and Defenses", Novembre 2023, Allemagne — Je n'ai pas pu y participer, étant en congé maternité
- Co-organisation de la journée "Security@CRISStAL", 2023, Lille, France
- Organisation de l'école d'été du GDR Sécurité, 2019, Rennes, France
- Publicité pour l'école de printemps Security & Correctness in the IoT 2017, Graz, Autriche
- Organisation sur site pour COSADE 2016, Graz, Autriche

Supervision d'étudiants

Thèses en cours (3)

- Iliana Fayolle, 2023-2026, "Side-channel vulnerabilities in Web environments"
 - Financement : ANR PRCI FACADES
 - Direction de thèse 100%
- Antoine Geimer, 2022-2025, "Détection automatique de vulnérabilités par canaux auxiliaires"
 - Financement : ANR JCJC MIAOUS + subvention AID
 - Encadrante principale, direction de thèse 50% avec Sandrine Blazy
 - Publication : [3]
- Pierre Ayoub, 2020-2023, "Security of IoT devices in 5G networks through fingerprinting and side-channel analysis"

- Financement : ANR PRCE MobiS5
- Co-encadrement 25% avec Aurélien Francillon et Romain Cayre
- Publication : [31]

Thèses soutenues (2)

- o Guillaume Didier, 2019-2022, "Studying hardware prefetchers using cache side channels"
 - Financement : IA DGA
 - Encadrante principale avec David Naccache (direction)
 - Publications : [10, 5]
 - Soutenance le 20 janvier 2023
- o Thomas Rokicki, 2019-2022, "Side Channels in Web Browsers: Applications to Security and Privacy"
 - Financement : ANR JCJC MIAOUS
 - Encadrante principale avec Gildas Avoine (direction)
 - Publications : [9, 7, 6, 4]
 - Soutenance le 29 novembre 2022

Postdocs (2)

- o Walid Ghandour, 2021-2023
- o Sam Thomas, 2018-2019

Étudiants de master (11)

Iliana Fayolle (M2 2023), Baptiste Demoussel (M1 2022), Rachida Saroui (M1 2022), Vibhakar Sivakumar (M1 2022), Antoine Geimer (M1 2021, M2 2022), Léo Cosseron (M1 2020), Pierre Ayoub (M2 2020), Julius Wenzel (M1 2020), Thibaut Perami (M1 2019), Thomas Rokicki (M2 2019), Lukas Giner (M2 2016)

Projets

- 2023–2027 PEPR Cybersécurité REV (responsable WP)
- 2022–2027 PEPR Cybersécurité iPoP (membre)
- 2022–2025 ANR-DFG PRCI FACADES (membre)
- 2019–2023 **ANR JCJC MIAOUS** (porteuse du projet)
- 2019–2023 ANR ARCHI-SEC (responsable scientifique IRISA)
- 2019–2023 ANR MobiS5 (membre)
- 2018 PEPS JCJC INS2I pour démarrer mon activité de recherche à l'IRISA
- 2018–2020 Financement DGA pour le recrutement d'un chercheur postdoctoral pour 2 ans

Prix

- 2023 **Most Influential DIMVA Paper 2014-2018** pour l'article [24]
- 2023 **Best Paper Award Runner-up** à la conférence DIMVA pour l'article [4]
- 2022 **Trophée Femme Cyber Chercheuse** à l'European Cyber Women Day
- 2022 **Première place au CSAW'22 Applied Research Competition MENA** pour l'article [8]
- 2018 **Prix Bretagne Jeune Chercheuse et Chercheur** dans la catégorie "Technologies de Pointe"
- 2015 **Best Paper Award** à la conférence DIMVA pour l'article [26]

Diffusion scientifique

J'ai présenté mes travaux de recherche dans des **séminaires d'équipes** internationales à l'occasion de visites, comme à Vienne ou à Bochum, ainsi que dans des **écoles de jeunes chercheurs**. Par ailleurs, deux **industriels** majeurs du domaine des micro-processeurs, à savoir Intel et Qualcomm, m'ont également invité à présenter mes travaux. Enfin, j'ai présenté mes travaux à des **conférences non académiques**, comme le Chaos Communication Congress, BlackHat Europe, ou les Rencontres Mondiales du Logiciel Libre. En effet, la communauté de sécurité organise beaucoup de conférences où les chercheurs académiques, industriels, ou plus généralement les passionnés peuvent se rencontrer. L'audience y est à la fois très large (12 000 personnes au Chaos Communication Congress de Hambourg) et également très diverse.

Suit une sélection de mes présentations, la liste complète est disponible sur ma page web: <https://cmaurice.fr>

- 2023 Keynote à la conférence PassTheSALT, Lille, France
Présentation plénière aux Journées Nationales du GDR Sécurité Informatique, Paris, France
- 2022 Keynote au symposium RAID 2022, Limassol, Chypre

- Cours invité à l'école d'été du GDR Sécurité "Cyber in Nancy", Nancy, France
 Cours invité à la Summer School on real-world crypto and privacy, Šibenik, Croatie
 Keynote à EuroSec 2022 (workshop co-localisé avec EuroSys), Rennes, France
 2021 Présentation invitée au 32e HP/HPE (Virtual) Colloquium On Information Security, virtuel
 Présentation invitée à la Journée Sécurité SIF, GDR Sécurité Informatique, RSD et SOC2, virtuel
 Panel "Experiment Artifact Sharing" du workshop LASER (NDSS'21), virtuel
 2020 Masterclass au Forum International de la Cybersécurité (FIC), Lille, France
 2019 Présentation invitée à la conférence FICHSA, Tel Aviv, Israel
 Cours invité à Ben-Gurion University of the Negev, Beer Sheva, Israel
 Présentation invitée à la journée sécurité, INSA Toulouse, France
 2018 Présentation invitée au 8th Inria/Technicolor Workshop On Systems (WOS8), Rennes, France
 Travaux pratiques à l'école d'été du GDR Sécurité "Cyber in Occitanie", Montpellier, France
 Présentation invitée au Colloque Architecture, Toulouse, France
 Présentation invitée aux journées nationales pré-GDR Sécurité Informatique, Paris, France
 2017 Présentation aux RMLL 2017, Saint-Étienne, France
 Présentation invitée au SSTIC 2017, Rennes, France
 Cours à l'école de printemps Security & Correctness in the IoT, Graz, Autriche
 Présentation à RuhrSec 2017, Bochum, Allemagne
 Keynote à XDOM0 2017 (workshop co-localisé avec EuroSys), Belgrade, Serbie
 Présentations invitées à Intel, Hillsboro, Oregon, USA
 Présentation invitée à Qualcomm, San Diego, Californie, USA
 2016 Présentation au Chaos Communication Congress (33C3), Hambourg, Allemagne
 Présentation invitée à SBA Research, Vienne, Autriche
 Cours invité au HackerPraktikum, Ruhr-University Bochum, Allemagne
 Présentation invitée à Ruhr-University Bochum, Allemagne
 Présentation à BlackHat Europe 2016, Londres, UK
 Cours invité à l'école d'été IPICS 2016 à KU Leuven, Belgique
 2015 Présentation au Chaos Communication Congress (32C3), Hambourg, Allemagne

Enseignement

- 2022 **Attaques par canaux auxiliaires**, *Polytech Lille*.
 Cours magistraux (30 étudiants, M2).
 (12h CM, 2022).
- 2020–2021 **Sécurité Matérielle**, *Centrale Supélec, Rennes*.
 Cours magistraux et travaux pratiques (5-30 étudiants, M2).
 (3h CM + 3h TP, 2020) & (3h CM, 2021).
- 2019–2020 **Sécurité**, *ENS Rennes*.
 Cours magistraux et création de 6 projets par binômes (12 étudiants, L3).
 (6h CM + 2h projet, 2019) & (6h CM + 4h projet, 2020).
- 2018–2021 **Attaques par canaux auxiliaires**, *INSA Rennes*.
 Cours magistraux et travaux pratiques (10-20 étudiants, M2).
 (10h CM + 6h TP, 2018-2019) & (10h CM, 2020-2021).
- 2017 **Projet veille technologique**, *Université de Rennes 1*.
 Projet de veille technologique sur les canaux cachés utilisant la micro-architecture (4 étudiants, M2). 19h.
- 2016, 2017 **Embedded security**, *TU Graz, Autriche*.
 Cours magistraux (en anglais). Participation à la création du cours, production et correction de l'examen final pour tous les étudiants (50 étudiants, master). 7.5h CM, 2016–2017.
- 2014 **Programmation orientée objet en Java**, *INSA Rennes*.
 Cours et travaux pratiques (groupe de 28 étudiants, L2). Correction hebdomadaire des travaux pratiques. Participation à la production et à la correction de l'examen final (110 étudiants). 14h TD + 14h TP.
- 2013 **Introduction à la programmation orientée objet en Java**, *INSA Rennes*.
 Cours et travaux pratiques (groupe de 29 étudiants, L1). Correction hebdomadaire des travaux pratiques. Participation à la production et à la correction de l'examen final (280 étudiants). 14h TD + 13h TP.