Prof. David Naccache
✉ 92 boulevard Suchet, 75016, Paris, France
French, single, born on February 21, 1967
🖷 david.naccache@ens.fr
☎ +33 (0)7.86.26.76.30

Professional experience

2015 to date Professor at École normale supérieure of Ulm Street (Exceptional class 2)[1]

Chair holder "Computer forensics", National Gendarmerie officers' school (EOGN)

Director of the ENS' forensic & cybersecurity research group of ÉNS[2]

Director of teaching in charge of the computer science admission program in computer science of ENS

2005 - 2015 Professor at Université Panthéon-Assas Paris II - PRES Sorbonne Universités

Creator and director of the Master 2 "Forensics of information systems" (EEJSI)[3]

Numerous PhDs directed in the areas of computer forensics information security & cryptology.

2007 Promotion (by CNU) to first class
2012 Promotion (by CNU) to the exceptional class 1
2014 Senior member of *Institut universitaire de France (first election)*
2016 Promotion (by the ÉNS' board) to the exceptional class 2
2020 Senior member of *Institut universitaire de France (second election)*

Other responsibilities

Forensic expert by the French Cour de cassation, previously expert by the International criminal court (Den Hague) and by the tribunals of Luxembourg. Nearly 50 forensic cases both civil and criminal.

Qualified member of the *Observatoire de la sécurité des moyens de paiement* de la Banque de France[4] (criminal response, fraud and regulation).

Several academic functions in France and abroad including e.g.:

2015-date	Honorary professor	Université de Luxembourg
2001-date	Advisory board member	Florida State University C-SAIT
2004-date	Visiting Professor	Royal Holloway University of London
2005-2007	Visiting Professor	University College London
2012	Visiting Fellow	Newton Institute, Cambridge GB
2014-date	Associate researcher	CRI, Université Panthéon-Sorbonne
2016-date	Invited professor	Xidian University, China
2004-2008	Advisory Professor	Beijing Jiaotong University, China

Education

2004 Research habilitation.
Director: Pr. Jacques Stern, Université Paris VII & École normale supérieure.
Jury chaired by Prof. Adi Shamir (Turing Award winner)
Professor qualification, CNU sections 26 and 27.

[1] The exceptional class 2 is the highest rank of university professors
[2] www.ens-paris.fr (5 researchers and 7 PhD candidates.)
[3] Master ranked "AAA" during 2 successive evaluation campaigns. The mark "AAA" is given to 4% of French masters.
[4] Qualified member. JORF n°0158 du 10/07/2009, n°0259 of 07/11/2012 and n°0147 of 24/06/2017.

1995	PhD, granted with highest honors Jury chaired by Whitfield Diffie (Turing Award winner) Director : Pr. Gérard Cohen, École nationale supérieure des télécommunications.
1990	IMAC, Université Panthéon-Assas Paris II. Granted with "Very good" mention.
1990	Master diploma, Université Paris VI.
1987	Undergraduate diploma (DEUG), Université Paris XIII.

Auditor of the national sessions of the National Institute for Advanced Studies in Security and Justice (INHESJ) and the Institute for Advanced Studies in National Defense (IHEDN, AED).

Industrial expérience

1993 - 2005 Gemalto (Gemplus International, 4000 employees in 2005).

1993 - 1999 :	Team manager Management of 3 persons
1999 - 2001 :	Group head Management of 35 persons
2001 - 2002 :	Department director Management of 60 persons
2002 - 2005 :	Division director Management of 70 persons

Executive functions at *Gemalto:*

2003 - 2005	VP – Security technologies & Risk Management
2005	SVP – Recherche & innovation

1992 - 1993	Philips Radioelectric & Telephonic Telecommunications Labs (Oberthur) Research Engineer
1990 - 1992	Thomson Consumer Electronics Advanced Research Labs (Technicolor) Research Engineer

Academic distinctions (partial list)

- *Doctor Honoris Causa* at Academia Tehnică Militară of Romania (2017), honorary professor at the l'University of Luxembourg (2015)[5].
- Prize « *Mentor Master of Science* » of the Royal institute of the work elites of Belgium (2015)[6]. Invited speaker at the Academy of sciences (Session of 24/03/2015) etc.
- World Intellectual Property Organization modelist[7]. Prolific inventor: 150 patent families (8 French inventors are authors of more than 110 patents[8]).
- Numerous industrial prizes including the RSA 2001 Industry Award and 2 Sesames Trophies 2004 (more than 250 million computers use the RFC 4226 Internet standard written by Pr. Naccache).
- Two letters of congratulation from the Military Governor of Paris, a letter of congratulation from the Major General of the National Gendarmerie and a testimony of satisfaction from the Commander of the IdF Region.
- Knight of the National Order of the Legion of Honor and of the National Order of Merit.
- Distinguished speaker[9] in more than 70 international scientific conferences.

[5] Decision B6-09/05/2015 of the Governance council of the University of Luxembourg

[6] To «*stimulate the high professional competency; the perfectioning of professional competency and the technical and and superior intellectual perfecting* ».

[7] WIPO is a UN agency

[8] http://bit.do/inventors, page 23

[9] *Distinguished speaker, keynote speaker* or *invited speaker*

- IACR Fellow, ESORICS Award winner, etc.
- Member or past member of large firm advisory boards: Technicolor, Huawei, Ingenico, Almerys, Altis Semiconductors, Spansion (a division of AMD) etc.

Works and publications

Auteur of more than 200 publications and inventor of about 170 patents.

Editorial duties in international journals (present and past, partial list)

International Journal of Psychology of Cyber Crime SERSC	Editor
International Journal of Information Security & Cybercrime IJISC	Editor
Security and Privacy Magazine IEEE	Editor
Computers & Security Elsevier	Editor
Security & Communications Networks Journal Wiley-Blackwell	Editor
Cybersecurity — Open Access Journal MDPI	Editor
Military Technical Academy Review Military Technical Academy (Roumanie)	Editor
International Journal of Reliable Information & Assurance KIISC	Editor
Small Scale Digital Device Forensics Journal Purdue University	Editor
Information Technologies Professional IEEE	Editor

PERSONAL BIBLIOGRAPHY

David Naccache

- H-index: 49
- Each entry is a different scientific result.
- ePrints, conferences and journal papers relating to the same result are grouped to avoid an inflation of references. monographs and authored textbooks are shown in other colors.

Publications in 2024

1. Aymene Mohammed Bouayed, Samuel Deslauriers-Gauthier, Adrian Iaccovelli, David Naccache.CNN Explainability with Multivector Tucker Saliency Maps for Self-Supervised Models. CoRR abs/2410.23072 (2024)

2. Leon Mächler, Gustav Grimberg, Ivan Ezhov, Manuel Nickel, Suprosanna Shit, David Naccache, Johannes C. Paetzold. FedPID: An Aggregation Method for Federated Learning. CoRR abs/2411.02152 (2024)

Publications in 2023

3. David Naccache, Ofer Yifrach-Stav. On Catalan Constant Continued Fractions. C2SI (2023): 43-54

4. Fatima-Ezzahra El Orche, Marcel Hollenstein, Sarah Houdaigoui, David Naccache, Daria Pchelina, Peter B. Rønne, Peter Y. A. Ryan, Julien Weibel, Robert Weil. Taphonomical Security: DNA Information with a Foreseeable Lifespan. FICC (2) 2023: 674-694

5. Aymene Mohammed Bouayed, Adrian Iaccovelli, David Naccache. Sampling From Autoencoders' Latent Space via Quantization And Probability Mass Function Concepts. IJCB 2023: 1-10

6. Vincent Giraud, David Naccache. Power Analysis Pushed too Far: Breaking Android-Based Isolation with Fuel Gauges. IWSEC 2023: 3-15

7. Hadrien Barral, Georges-Axel Jaloyan, David Naccache. Emoji shellcoding in RISC-V. SP (Workshops) 2023: 255-263

8. David Naccache, Ofer Yifrach-Stav. Pattern Recognition Experiments on Mathematical Expressions. CoRR abs/2301.01624 (2023)

9. Aymene Mohammed Bouayed, David Naccache. Simplex Autoencoders. CoRR abs/2301.06489 (2023)

10. Aymene Mohammed Bouayed, Adrian Iaccovelli, David Naccache. Sampling From Autoencoders' Latent Space via Quantization And Probability Mass Function Concepts. CoRR abs/2308.10704 (2023)

11. Vincent Giraud, David Naccache. Bypassing Android isolation with fuel gauges: new risks with advanced power ICs. IACR Cryptol. ePrint Arch. 2023: 1078 (2023)

12. Houda Ferradi, Antoine Houssais, David Naccache. How to Physically Hold Your Bitcoins ? IACR Cryptol. ePrint Arch. 2023: 1485 (2023)

13. Rémi Géraud-Stewart, David Naccache. New Public-Key Cryptosystem Blueprints Using Matrix Products in 픽p. IACR Cryptol. ePrint Arch. 2023: 1745 (2023)

14. Julien S. Jainsky, David Naccache, Bassem Ouni, Ofer Yifrach-Stav. Authenticating Medications with QR-Codes and Compact Digital Signatures. IACR Cryptol. ePrint Arch. 2023: 1817 (2023)

15. Rémi Géraud-Stewart, David Naccache, Ofer Yifrach-Stav. Fiat-Shamir Goes Tropical. IACR Cryptol. ePrint Arch. 2023: 1954 (2023)

16. David Naccache, Ofer Yifrach-Stav. On The Practical Advantage of Committing Challenges in Zero-Knowledge Protocols. IACR Cryptol. ePrint Arch. 2023: 1961 (2023)

Publications in 2022

17. Hadrien Barral, Georges-Axel Jaloyan, Fabien Thomas-Brans, Matthieu Regnery, Rémi Géraud-Stewart, Thibaut Heckmann, Thomas Souvignet, David Naccache. A forensic analysis of the Google Home: repairing compressed data without error correction. arXiv:2210.00856 and Forensic Science International: Digital Investigation, Volume 42, 2022

18. Jean-Max Dutertre, Amir-Pasha Mirbaha, David Naccache, Assia Tria: *Photonic Power Firewalls*. Festschrift for David Kahn volume. Springer LNCS 9100 (The New Codebreakers 2016: 342-354) and J. Cryptogr. Eng. 12(3): 245-254 (2022)

19. Gergei Bana, Marco Biroli, Megi Dervishi, Fatima-Ezzahra El Orche, Rémi Géraud-Stewart, David Naccache, Peter B. Rønne, Peter Y. A. Ryan, Hugo Waltsburger: Time, Privacy, Robustness, Accuracy: Trade Offs for the Open Vote Network Protocol. IACR Cryptol. ePrint Arch. 2021: 1065 (2021) and E-Vote-ID 2022: 19-35

20. Adnan Ben Mansour, Gaia Carenini , Alexandre Duplessis, David Naccache: Federated Learning Aggregation: New Robust Algorithms with Guarantees. CoRR abs/2205.10864 (2022) accepted to the 21st IEEE International conference on machine learning and applications (IEEE ICMLA 2022)

21. Adnan Ben Mansour, Gaia Carenini , Alexandre Duplessis, David Naccache: FedControl: When Control Theory Meets Federated Learning. CoRR abs/2205.14236 (2022) appeared in New in ML workshop at ICML 2022

22. Leon Mächler, David Naccache: A Conjecture on Hermite Constants. IACR Cryptol. ePrint Arch. 2022: 677 (2022)

23. David Naccache, Ofer Yifrach-Stav: Invisible Formula Attacks. IACR Cryptol. ePrint Arch. 2022: 1110 (2022) also BlackHat 2022.

24. David Naccache, Ofer Yifrach-Stav: On Squaring Modulo Mersenne Numbers. IACR Cryptol. ePrint Arch. 2022: 1197 (2022)

25. David Naccache, Ofer Yifrach-Stav: A Conjecture From a Failed Cryptanalysis. IACR Cryptol. ePrint Arch. 2022: 1273 (2022)

Publications in 2021

26. Théodore Conrad-Frenkiel, Rémi Géraud-Stewart, David Naccache: On Unpadded NTRU Quantum (In)Security. IACR Cryptol. ePrint Arch. 2021: 1426 (2021) and 46th Wireless World Research Forum.

27. Carlton Shepherd, Konstantinos Markantonakis, Nico van Heijningen, Driss Aboulkassimi, Clément Gaine, Thibaut Heckmann, David Naccache: Physical fault injection and side-channel attacks on mobile devices: A comprehensive analysis. Comput. Secur. 111: 102471 (2021) et CoRR abs/2105.04454 (2021)

28. Thibaut Heckmann, Thomas R. Souvignet, Damien Sauveron, David Naccache: Medical Equipment Used for Forensic Data Extraction: A low-cost solution for forensic laboratories not provided with expensive diagnostic or advanced repair equipment. Digit. Investig. 36(Supplement): 301092 (2021)

29. Fatima-Ezzahra El Orche, Marcel Hollenstein, Sarah Houdaigoui, David Naccache, Daria Pchelina, Peter B. Rønne, Peter Y. A. Ryan, Julien Weibel, Robert Weil: Taphonomical Security: (DNA) Information with Foreseeable Lifespan. IACR Cryptol. ePrint Arch. 2021: 1066 (2021)

30. Eric Brier, Rémi Géraud-Stewart, Marc Joye, David Naccache: Primary Elements in Cyclotomic Fields with Applications to Power Residue Symbols, and More. IACR Cryptol. ePrint Arch. 2021: 1106 (2021) Gergei Bana, Wojciech Jamroga, David Naccache, Peter Y. A. Ryan: Convergence Voting: From Pairwise Compari- sons to Consensus. CoRR abs/2102.01995 (2021)

31. Leon Mächler, David Naccache: Explaining the Entombed Algorithm. CoG 2021: 1-4 et CoRR abs/2104.09982 (2021)

32. Éric Brier, Megi Dervishi, Rémi Géraud-Stewart, David Naccache, Ofer Yifrach-Stav: Near-Optimal Pool Testing under Urgency Constraints. CoRR abs/2106.10971 (2021)

33. Antoine Scardigli, Paul Fournier, Matteo Vilucchio, David Naccache Genealogical Population-Based Training for Hy-

perparameter Optimization. arXiv:2109.14925. 2021.

34. Rémi Géraud-Stewart, David Naccache: Magnetic RSA. IACR Cryptol. ePrint Arch. 2021: 77 (2021)

35. Hadrien Barral, Éric Brier, Rémi Géraud-Stewart, Arthur Léonard, David Naccache, Quentin Vermande, Samuel Vivien: Discovering New L-Function Relations Using Algebraic Sieving. IACR Cryptol. ePrint Arch. 2021: 1060 (2021)

36. Gaëlle Candel, David Naccache: Tagged Documents Co-Clustering. CoRR abs/2110.11079 (2021) and 2021 World Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE'21) - track ICAI21

37. Eric Brier, Christophe Clavier, Linda Gutsche, David Naccache. The Multiplicative Persistence Conjecture Is True for Odd Targets. CoRR abs/2110.04263. 2021.

38. Gaëlle Candel, David Naccache: Co-Embedding: Discovering Communities on Bipartite Graphs through Projection. CoRR abs/2109.07135 (2021). FICC 2022 (Future of Information and Communication Conference)

39. Gaëlle Candel, David Naccache: Generating Local Maps of Science using Deep Bibliographic Coupling. CoRR abs/2109.10007 (2021) July 12-15, 2021. 18th International Conference of the International Society for Scientometrics and Informetrics Leuven, Belgium

40. Gaëlle Candel, David Naccache: Index t-SNE: Tracking Dynamics of High-Dimensional Datasets with Coherent Embeddings. CoRR abs/2109.10538 (2021). International Conference on Big Data Visual Analytics (ICBDVA), Venice, Italy, August 12-13, 2021 (best paper award) and International Journal of Computer and Systems Engineering (2021), 15(8), 500 - 512

41. Gaëlle Candel, David Naccache: Noise-Resilient Ensemble Learning using Evidence Accumulation Clustering. CoRR abs/2110.09212 (2021) appeared at ANTIC-2021 (International Conference on Advanced Network Technologies and Intelligent Computing)

42. Marc Joye, Oleksandra Lapiha, Ky Nguyen, David Naccache: The Eleventh Power Residue Symbol, IACR Cryptology ePrint Archive 2019: 870 (2019). Journal of Mathematical Cryptology. 15(1): 111-122 (2021)

43. Clémence Chevignard, Rémi Géraud-Stewart, Antoine Houssais, David Naccache, Edmond de Roffignac: How to Claim a Computational Feat. IACR Cryptol. ePrint Arch. 2021: 1554 (2021)

44. Georges-Axel Jaloyan, Konstantinos Markantonakis, Raja Naeem Akram, David Robin, Keith Mayes, David Naccache: Return-Oriented Programming on RISC-V. AsiaCCS 2020: 471-480 and CoRR abs/2103.08229 (2021)

45. Rémi Géraud-Stewart, David Naccache: Elementary Attestation of Cryptographically Useful Composite Moduli. SECITC 2020: 1-12 et IACR Cryptol. ePrint Arch. 2021: 52 (2021)

Publications in 2020

46. Marcel Hollenstein, David Naccache, Peter B. Rønne, Peter Y. A. Ryan, Robert Weil, Ofer Yifrach-Stav: Preservation of DNA Privacy During the Large-Scale Detection of COVID 19. IACR Cryptol. ePrint Arch. 2021: 1108 (2021) et CoRR abs/2007.09085 (2020)

47. David Naccache, Rémi Géraud: Invited Talk: A French Code from the Late 19th Century. HistoCrypt 2018: 149:003 and Cryptologia 45(4): 342-370 (2021) and IACR Cryptol. ePrint Arch. 2020: 390 (2020).

48. Houda Ferradi, Rémi Géraud, Sylvain Guilley, David Naccache, Mehdi Tibouchi: Recovering Secrets From Prefix-Dependent Leakage. J. Math. Cryptol. 14(1): 15-24 (2020) and IACR Cryptol. ePrint Arch. 2018: 798 (2018)

49. Jean-Claude Caraco, Rémi Géraud-Stewart, David Naccache: Kerckhoffs' Legacy. IACR Cryptol. ePrint Arch. 2020: 556 (2020)

50. Marc Beunardeau, Éric Brier, Noémie Cartier, Aisling Connolly, Nathanaël Courant, Rémi Géraud-Stewart, David Naccache, Ofer Yifrach-Stav: Optimal Covid-19 Pool Testing with a priori Information. CoRR abs/2005.02940 (2020)

51. Guillaume Bertholon, Rémi Géraud-Stewart, Axel Kugelmann, Théo Lenoir, David Naccache: At Most 43 Moves, At Least 29: Optimal Strategies and Bounds for Ultimate Tic-Tac-Toe. CoRR abs/2006.02353 (2020)

52. Éric Brier, Rémi Géraud-Stewart, David Naccache, Alessandro Pacco, Emanuele Troiani: Stuttering Conway Sequences Are Still Conway Sequences. CoRR abs/2006.06837 (2020)

53. Éric Brier, Rémi Géraud-Stewart, David Naccache, Alessandro Pacco, Emanuele Troiani: The Look-and-Say The Biggest Sequence Eventually Cycles. CoRR abs/2006.07246 (2020)

54. Éric Brier, Rémi Géraud-Stewart, David Naccache: A Fractional 3n+1 Conjecture. CoRR abs/2006.11634 (2020)

55. Rémi Géraud-Stewart, Marius Lombard-Platet, David Naccache: Approaching Optimal Duplicate Detection in a Sliding Window. COCOON 2020: 64-84 et CoRR abs/2005.04740 (2020)

56. Hadrien Barral, Rémi Géraud-Stewart, Amaury Barral, David Naccache. DNSSECTION: A practical attack on DNSSEC Zone Walking, Defcon 28. https://dnssection.ovh/

Publications in 2019

57. Éric Brier, Houda Ferradi, Marc Joye, David Naccache: New number-theoretic cryptographic primitives. J. Math. Cryptol. 14(1): 224-235 (2020) et IACR Cryptol. ePrint Arch. 2019: 484 (2019)

58. Marc Beunardeau, Fatima-Ezzahra El Orche, Diana Maimut, David Naccache, Peter B. Rønne, Peter Y. A. Ryan: Authenticated Key Distribution: When the Coupon Collector is Your Enemy. SECITC 2019: 1-20 et IACR Cryptol. ePrint Arch. 2019: 1499 (2019)

59. Eric Brier, David Naccache: The Thirteenth Power Residue Symbol. IACR Cryptol. ePrint Arch. 2019: 1176 (2019)

60. Thibaut Heckmann, Thomas Souvignet, David Naccache: Decrease of energy deposited during laser decapsulation attacks by dyeing and pigmenting the ECA: Application to the forensic micro-repair of wire bonding. Digital Investigation 29: 210-218 (2019)

61. Thibaut Heckmann, James P. McEvoy, Konstantinos Markantonakis, Raja Naeem Akram, David Naccache: Removing epoxy underfill between neighbouring components using acid for component chip-off. Digital Investigation 29: 198-209 (2019).

62. Yao Cheng, Cheng-Kang Chu, Hsiao-Ying Lin, Marius Lombard-Platet, David Naccache, Keyed Non-Parametric Hypothesis Tests, Protecting Machine Learning From Poisoning Attacks, 13th International Conference on Network and System Security NSS 2019: 632-645 et CoRR abs/2005.12227 (2020)

63. Houda Ferradi, David Naccache: Integer Reconstruction Public-Key Encryption. IACR Cryptology ePrint Archive 2017: 1231 (2017). CANS 2019: 412-433.

64. Rémi Géraud, David Naccache, Razvan Rosie: Robust Encryption, Extended. CT-RSA 2019: 149-168. IACR Cryptology ePrint Archive 2019: 238 (2019)

65. Rémi Géraud, Marius Lombard-Platet, David Naccache: Quotient hash tables: efficiently detecting duplicates in streaming data. SAC 2019: 582-589. CoRR abs/1901.04358 (2019)

66. Gaëlle Candel, Rémi Géraud-Stewart, David Naccache: How to Compartment Secrets. WISTP 2019: 3-11 et IACR Cryptol. ePrint Arch. 2019: 1397 (2019)

67. Hadrien Barral, Rémi Géraud-Stewart, Georges-Axel Jaloyan, David Naccache: RISC-V: #Alphanumeric Shellcoding. WOOT, USENIX Security Symposium 2019. CoRR abs/1908.03819 (2019)

68. Marc Beunardeau, Houda Ferradi, Rémi Géraud, David Naccache: *Honey Encryption for Language*. IACR Cryptology ePrint Archive 2017: 31 (2017)

69. Eric Brier, Houda Ferradi, Marc Joye, David Naccache: New Number-Theoretic Cryptographic Primitives. IACR Cryptology ePrint Archive 2019: 484 (2019). Journal of Mathematical Cryptology.

Publications in 2018

70. Weiran Liu, Jianwei Liu, Qianhong Wu, Bo Qin, David Naccache, Houda Ferradi: Compact CCA2-secure Hierarchical Identity-Based Broadcast Encryption for Fuzzy-Entity Data Sharing. IACR Cryptology ePrint Archive 2016: 634 (2016) Efficient Subtree-Based Encryption for Fuzzy-Entity Data Sharing. Soft Comput. 22(23): 7961-7976 (2018)

71. Rémi Géraud, David Naccache: Mixed-radix Naccache-Stern Encryption. J. Cryptographic Engineering 9(3): 277-282 (2019) IACR Cryptology ePrint Archive 2018: 278 (2018)

72. Houda Ferradi, Rémi Géraud, Diana Maimut, David Naccache, Hang Zho, Backtracking-Assisted Multiplication IACR Cryptology ePrint Archive 2015: 787 (2015). Arctic Crypt 2016. Cryptography and Communications 10(1): 17-26 (2018)

73. Houda Ferradi, Rémi Géraud, Diana Maimut, David Naccache, Amaury de Wargny: Regulating the Pace of von Neumann Correctors. IACR Cryptology ePrint Archive 2015: 849 (2015). Journal of Cryptographic Engineering . 8(1): 85-91 (2018)

74. Thibaut Heckmann, Konstantinos Markantonakis, David Naccache, Thomas R. Souvignet: Forensic smartphone analysis using adhesives: Transplantation of Package-on-Package components. Digit. Investig. 26: 29-39 (2018)

75. Simon Cogliani, Feng Bao, Houda Ferradi, Rémi Géraud, Diana Maimut, David Naccache, Rodrigo Portella do Canto, Guilin Wang: *Public-Key Based Lightweight Swarm Authentication*. IACR Cryptology ePrint Archive 2016: 750 (2016) and Cyber-Physical Systems Security 2018: 255-267

Publications in 2017

76. Thibaut Heckmann, Thomas Souvignet, David Naccache: Electrically conductive adhesives, thermally conductive adhesives and UV adhesives in data extraction forensics. Digital Investigation 21: 53-64 (2017)

77. Rémi Géraud, Mirko Koscina, Paul Lenczner, David Naccache, David Saulpic: Generating Functionally Equivalent Programs Having Non-Isomorphic Control-Flow Graphs. CoRR abs/1709.08357 (2017) and NordSec 2017: 265-279

78. Marc Beunardeau, Aisling Connolly, Rémi Géraud, David Naccache: On the Hardness of the Mersenne Low Hamming Ratio Assumption. IACR Cryptology ePrint Archive 2017: 522 (2017). LATINCRYPT 2017: 166-174

79. Rémi Géraud and David Naccache and Răzvan Roşie: Twisting Lattice and Graph Techniques to Compress Transactional Ledgers. IACR Cryptology ePrint Archive 2017: 751 (2017). SecureComm'17: 108-127.

80. Marc Beunardeau, Aisling Connolly, Rémi Géraud, David Naccache: The Case for System Command Encryption. AsiaCCS 2017: 6

81. Eric Brier, Rémi Géraud, David Naccache: Exploring Naccache-Stern Knapsack Encryption. IACR Cryptology ePrint Archive 2017: 421 (2017) SECITC 2017: 67-82

82. Fabrice Benhamouda, Houda Ferradi, Rémi Géraud, David Naccache: Non-Interactive Provably Secure Attestations for Arbitrary RSA Prime Generation Algorithms. IACR Cryptology ePrint Archive 2017: 640 (2017). Also ESORICS 2017: 206-223

83. Marc Beunardeau, Aisling Connolly, Rémi Géraud, David Naccache and Damien Vergnaud. Reusing Nonces in Schnorr Signatures- (and Keeping It Secure...). ESORICS 2017: 224-241. Also IACR Cryptology ePrint Archive 2018: 69 (2018)

Publications in 2016

84. Thibaut Heckmann, Thomas Souvignet, Sébastien Lepeer, David Naccache: Low-temperature low-cost 58 Bismuth - 42 Tin alloy forensic chip re-balling and re-soldering. Digital Investigation 19: 60-68 (2016)

85. Peter Y. A. Ryan, David Naccache, Jean-Jacques Quisquater: *The New Codebreakers - Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Lecture Notes in Computer Science 9100, Springer 2016, ISBN 978-3-662-49300-7

86. Simon Cogliani, Houda Ferradi, Rémi Géraud, David Naccache: Thrifty Zero-Knowledge - When Linear Programming Meets Cryptography. IACR Cryptology ePrint Archive 2016: 443 (2016). ISPEC 2016: 344-353

87. Ehsan Aerabi, A. Elhadi Amirouche, Houda Ferradi, Rémi Géraud, David Naccache, Jean Vuillemin: The Conjoined Microprocessor. IACR Cryptology ePrint Archive 2015: 974 (2015). HOST 2016: 67-70

88. Houda Ferradi, Rémi Géraud, Diana Maimut, David Naccache, David Pointcheval: Legally Fair Contract Signing Without Keystones. IACR Cryptology ePrint Archive 2016: 363 (2016) and ACNS 2016: 175-190

89. Hadrien Barral, Houda Ferradi, Rémi Géraud, Georges-Axel Jaloyan, David Naccache: ARMv8 Shellcodes from 'A' to 'Z'. ISPEC 2016: 354-377. CoRR abs/1608.03415 (2016)

90. Marc Beunardeau, Aisling Connolly, Rémi Géraud, David Naccache: *White-Box Cryptography: Security in an Insecure Environment*. IEEE Security & Privacy 14(5): 88-92 (2016)

91. Marc Beunardeau, Aisling Connolly, Rémi Géraud, David Naccache: Fully Homomorphic Encryption: Computations with a Blindfold. IEEE Security & Privacy 14(1): 63-67 (2016).

92. Marc Beunardeau, Aisling Connolly, Rémi Géraud, David Naccache: Cdoe Obofsucaitn: Securing Software from Within. IEEE Security & Privacy 14(3): 78-81 (2016)

93. Houda Ferradi, Rémi Géraud, David Naccache, Assia Tria: When Organized Crime Applies Academic Results - A Forensic Analysis of an In-Card Listening Device. IACR Cryptology ePrint Archive 2015: 963 (2015). J. of Cryptographic Engineering 6(1): 49-59 (2016).

94. Jean-Sébastien Coron, David Naccache, Mehdi Tibouchi, Ralf-Philipp Weinmann: *Practical Cryptanalysis of ISO/IEC 9796-2 and EMV Signatures*. CRYPTO 2009: 428-444 and IACR Cryptology ePrint Archive 2009: 203 (2009). J. Cryptology 29(3): 632-656 (2016).

95. Houda Ferradi, Rémi Géraud, David Naccache: *Human Public-Key Encryption*. IACR Cryptology ePrint Archive 2016: 763 (2016)

96. Simon Cogliani, Rémi Géraud, David Naccache: *A Fiat-Shamir Implementation Note*. IACR Cryptology ePrint Archive 2016: 1039 (2016)

97. Jean-Michel Cioranesco, Houda Ferradi, Rémi Géraud, David Naccache: *Process Table Covert Channels: Exploitation and Countermeasures*. IACR Cryptology ePrint Archive 2016: 227 (2016)

98. Gildas Barbier, Sandrine Parise-Heideiger, Alexis Mihman, Justine Aubriot, Christophe Barret, Saïd Belhacen, David Book, Magali Caillat, Maria Jesus Cantos Cebrian, Sébastien Cetti, Stéphanie Desjars, Cynthia Fabre, Christian Goyheneix, David Naccache, Stéphane de Paoli, Didier Rémond, *Pour une enquête pénale plus efficace - Les évolutions possibles face aux menaces nouvelles et au formalisme croissant issu notamment du droit européen*. Institut national des hautes études de la sécurité et de la justice (2016)

Publications in 2015

99. Bo Qin, Hua Deng, Qianhong Wu, Josep Domingo-Ferrer, David Naccache, Yunya Zhou, Flexible Attribute-Based Encryption Applicable to Secure E-Healthcare Records, International Journal of Information Security 14(6): 499-511 (2015) CoRR abs/1512.06578 (2015).

100. Jérémie Clément, Bruno Mussard, David Naccache, Lionel Torres: Implementation of AES Using NVM Memories Based on Comparison Function. ISVLSI 2015: 356-361

101. Houda Ferradi, Rémi Géraud, David Naccache: Slow Motion Zero Knowledge Identifying With Colliding Commitments. IACR Cryptology ePrint Archive 2016: 399 (2016). Inscrypt 2015: 381-396

102. Diana Maimut, David Naccache, Rodrigo Portella do Canto, Emil Simion Applying Cryptographic Acceleration Techniques to Error Correction, Proceedings of SECITC 2015, Springer LNCS 2015. 150-168. IACR Cryptology ePrint Archive 2015: 886 (2015).

103. Eric Brier, Jean-Sébastien Coron, Rémi Géraud, Diana Maimut, David Naccache, A Number-Theoretic Error-Correcting Code, Proceedings of SECITC 2015: 25-35, LNCS 2015. CoRR abs/1509.00378 (2015)

104. Céline Chevalier, Damien Gaumont, David Naccache, Rodrigo Portella do Canto, *How to (Carefully) Breach a Service Contract?*, Festschrift for David Kahn volume. Springer LNCS 9100 (The New Codebreakers 2016: 166-173).

105. Jean-Michel Cioranesco, Roman Korkikian, David Naccache, Rodrigo Portella do Canto, AES Design Resistance with Speed and Energy, IACR Cryptology ePrint Archive 2015: 768 (2015). Festschrift for David Kahn volume. Springer LNCS 9100 (The New Codebreakers 2016: 134-147).

106. Pierre-Alain Fouque, Sylvain Guilley, Cédric Murdica, David Naccache, *Safe-Errors on SPA Protected implementations with the Atomicity Technique*, IACR Cryptology ePrint Archive 2015: 764 (2015). Festschrift for David Kahn volume. Springer LNCS 9100 (The New Codebreakers 2016: 479-493).

107. Antoine Amarilli, Marc Beunardeau, Rémi Géraud, David Naccache: Failure is Also an Option. Festschrift for David Kahn volume. Springer. Springer LNCS 9100. Springer LNCS 9100 The New Codebreakers 2016: 161-165

108. Jean-Luc Danger, Sylvain Guilley, Philippe Hoogvorst, Cédric Murdica, David Naccache, Improving the Big Mac Attack on Elliptic Curve Cryptography. Festschrift for David Kahn volume. Springer LNCS 9100 (The New Codebreakers 2016: 374-386). IACR Cryptology ePrint Archive 2015: 819 (2015)

109. Rémi Géraud, Diana Maimut, David Naccache, Double-Speed Barrett Moduli, IACR Cryptology ePrint Archive 2015: 785 (2015). Festschrift for David Kahn volume. Springer LNCS 9100 (The New Codebreakers 2016: 148-158).

110. Thierry Leclercq, Olivier Mahler, Marcel David, Sébastien Berthomieu, Raphaël Cuisinier, Patrice Maillard, David Naccache, Alexandre Nimser, Vincent Pery, Gilles Foultier, *Les missiles hypervéloces : entre mythe et réalité ?*, IHEDN, Regards AED 2014-2015.

Publications in 2014

111. Roman Korkikian, Sylvain Pelissier, David Naccache: *Blind Fault Attack against SPN Ciphers*. FDTC 2014: 94-103

112. Mehari Msgna, Konstantinos Markantonakis, David Naccache, Keith Mayes: *Verifying Software Integrity in Embedded Systems: A Side Channel Approach.* COSADE 2014: 261-280

113. Jean-Michel Cioranesco, Jean-Luc Danger, Tarik Graba, Sylvain Guilley, Yves Mathieu, David Naccache, Xuan Thuy Ngo: *Cryptographically secure shields*. HOST 2014: 25-31

114. Michel Abdalla, Hervé Chabanne, Houda Ferradi, Julien Jainski, David Naccache: *Improving Thomlinson-Walker's Software Patching Scheme Using Standard Cryptographic and Statistical Tools*. ISPEC 2014: 8-14

115. Simon Cogliani, Diana-Stefania Maimut, David Naccache, Rodrigo Portella do Canto, Reza Reyhanitabar, Serge Vaudenay, Damian Vizár: *OMD: A Compression Function Mode of Operation for Authenticated Encryption*. Selected Areas in Cryptography 2014: 112-128

116. David Naccache, Rainer Steinwandt, Adriana Suárez Corona, Moti Yung: *Narrow Bandwidth Is Not Inherent in Reverse Public-Key Encryption*. SCN 2014: 598-607

117. Thomas Bourgeat, Julien Bringer, Hervé Chabanne, Robin Champenois, Jérémie Clément, Houda Ferradi, Marc Heinrich, Paul Melotti, David Naccache, Antoine Voizard: *New Algorithmic Approaches to Point Constellation Recognition*. IFIP SEC 2014: 80-90 and CoRR abs/1405.1402 (2014)

Publications in 2013

118. Jean-Michel Cioranesco, Houda Ferradi, David Naccache, Communicating covertly through CPU monitoring. IEEE Security & Privacy. Security & Privacy, IEEE, Volume 11 Issue 6, pp. 71–73, 2013

119. Jean-Luc Danger, Sylvain Guilley, Philippe Hoogvorst, Cédric Murdica, David Naccache: *Dynamic countermeasure against the Zero Power Analysis*. ISSPIT 2013: 140-147 and IACR Cryptology ePrint Archive 2013: 764 (2013)

120. Hervé Chabanne, Jean-Michel Cioranesco, Vincent Despiegel, Jean-Christophe Fondeur, David Naccache, *Using Hamiltonian Totems as Passwords*, SantaCrypt'2013 and IACR Cryptology ePrint Archive 2013: 751 (2013)

121. Diana Maimut, Cédric Murdica, David Naccache, Mehdi Tibouchi: *Fault Attacks on Projective-to-Affine Coordinates Conversion*. COSADE 2013: 46-61

122. Roman Korkikian, David Naccache, Guilherme Ozari de Almeida: *Instantaneous Frequency Analysis*. IACR Cryptology ePrint Archive 2013: 320 (2013) and DCNET/ICE-B/OPTICS 2013: IS-11 followed-up by experimental results in [same authors] + Rodrigo Portella do Canto: *Practical Instantaneous Frequency Analysis Experiments*. ICETE (Selected Papers) 2013: 17-34

123. Jean-Luc Danger, Sylvain Guilley, Philippe Hoogvorst, Cédric Murdica, David Naccache: *A synthesis of side-channel attacks on elliptic curve cryptography in smart-cards*. J. Cryptographic Engineering 3(4): 241-265 (2013)

124. Eric Brier, David Naccache, Li-yao Xia: *How to Sign Paper Contracts? Conjectures & Evidence Related to Equitable & Efficient Collaborative Task Scheduling*. IACR Cryptology ePrint Archive 2013: 432 (2013) and Chapter in the book Open Problems in Mathematics and Computational Science, Springer, pp 317-340.

Publications in 2012

125. Eric Brier, Wenjie Fang, David Naccache: How to Scatter a Secret? Cryptologia 36(1): 46-54 (2012)

126. David Naccache, David Pointcheval: Autotomic Signatures. Cryptography and Security 2012: 143-155

127. Byungchun Chung, Sandra Marcello, Amir-Pasha Mirbaha, David Naccache, Karim Sabeg: *Operand Folding Hardware Multipliers*. Cryptography and Security 2012: 319-328 and CoRR abs/1104.1533 (2011)

128. Guillaume Claret, Michaël Mathieu, David Naccache, Guillaume Seguin: *Physical Simulation of Inarticulate Robots*. Cryptography and Security 2012: 491-499 and CoRR abs/1104.1546 (2011)

129. Alessandro Barenghi, Luca Breveglieri, Israel Koren, David Naccache: Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures. Proceedings of the IEEE 100(11): 3056-3076 (2012)

130. Jean-Luc Danger, Sylvain Guilley, Philippe Hoogvorst, Cédric Murdica, David Naccache: *Low-Cost Countermeasure against RPA*. CARDIS 2012: 106-122

131. Eric Brier, Quentin Fortier, Roman Korkikian, K. W. Magld, David Naccache, Guilherme Ozari de Almeida, Adrien Pommellet, A. H. Ragab, Jean Vuillemin: *Defensive Leakage Camouflage*. CARDIS 2012: 277-295 and IACR Cryptology ePrint Archive 2012: 728 (2012) and IACR Cryptology ePrint Archive 2012: 324 (2012)

132. Sébastien Briais, Stéphane Caron, Jean-Michel Cioranesco, Jean-Luc Danger, Sylvain Guilley, Jacques-Henri Jourdan, Arthur Milchior, David Naccache, Thibault Porteboeuf: *3D Hardware Canaries*. CHES 2012: 1-22

133. Cédric Murdica, Sylvain Guilley, Jean-Luc Danger, Philippe Hoogvorst, David Naccache: *Same Values Power Analysis Using Special Points on Elliptic Curves*. COSADE 2012: 183-198

134. Jean-Sébastien Coron, David Naccache, Mehdi Tibouchi: *Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers*. EUROCRYPT 2012: 446-464

135. Sébastien Briais, Jean-Michel Cioranesco, Jean-Luc Danger, Sylvain Guilley, David Naccache, Thibault Porteboeuf: *Random Active Shield*. FDTC 2012: 103-113

136. Jean-Max Dutertre, Amir-Pasha Mirbaha, David Naccache, Anne-Lise Ribotta, Assia Tria, Thierry Vaschalde: *Fault Round Modification Analysis of the Advanced Encryption Standard*. HOST 2012: 140-145

137. Antoine Amarilli, Fabrice Ben Hamouda, Florian Bourse, Robin Morisset, David Naccache, Pablo Rauzy: *From Rational Number Reconstruction to Set Reconciliation and File Synchronization*. TGC 2012: 1-18

138. David Naccache (Ed.): *Cryptography and Security: From Theory to Applications - Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday*. Lecture Notes in Computer Science 6805, Springer 2012, ISBN 978-3-642-28367-3

139. Jean-Sébastien Coron, David Naccache, Mehdi Tibouchi: *Another Look at Affine-Padding RSA Signatures*. ICISC 2012: 22-32 and IACR Cryptology ePrint Archive 2011: 57 (2011)

Publications in 2011

140. Eric Brier, David Naccache, Phong Q. Nguyen, Mehdi Tibouchi: *Modulus fault attacks against RSA-CRT signatures*. J. Cryptographic Engineering 1(3): 243-253 (2011) and CHES 2011: 192-206 and IACR Cryptology ePrint Archive 2011: 388 (2011)

141. Jean-Sébastien Coron, Antoine Joux, Avradip Mandal, David Naccache, Mehdi Tibouchi: *Cryptanalysis of the RSA Subgroup Assumption from TCC 2005*. Public Key Cryptography 2011: 147-155 and IACR Cryptology ePrint Archive 2010: 650 (2010)

142. Jean-Sébastien Coron, Avradip Mandal, David Naccache, Mehdi Tibouchi: *Fully Homomorphic Encryption over the Integers with Shorter Public Keys*. CRYPTO 2011: 487-504 and IACR Cryptology ePrint Archive 2011: 441 (2011)

143. Antoine Amarilli, David Naccache, Pablo Rauzy, Emil Simion: *Can a Program Reverse-Engineer Itself?* IMA Int. Conf. 2011: 1-9 and IACR Cryptology ePrint Archive 2011: 497 (2011)

144. Antoine Amarilli, Sascha Müller, David Naccache, Dan Page, Pablo Rauzy, Michael Tunstall: *Can Code Polymorphism Limit Information Leakage?* WISTP 2011: 1-21 and IACR Cryptology ePrint Archive 2011: 99 (2011)

145. D. Naccache, E. Simion, A. Mihăiță, R.-F. Olimid, A.-G. Oprina. *Criptografie si securitatea informatiei. Aplicatii.*, 107 pages, Matrix Rom, 2011.

146. Jean-Sébastien Coron, David Naccache, Mehdi Tibouchi: *Optimization of Fully Homomorphic Encryption*. IACR Cryptology ePrint Archive 2011: 440 (2011)

147. E. Simion, M. Andrașiu, D. Naccache, G. Simion. *Cercetări operaționale,probabilități si criptologie. Aplicatii.*, 292 pages, Editura Academiei Tehnice Militare, 2011.

148. David Naccache: Encyclopedia of Cryptography and Security (2nd Ed.) 2011 entries:

Autotomic Signatures	*Multiplicative Knapsack*
Barrett's Algorithm	*Naccache-Stern Higher Residues Cryptosystem*
Blackmailing Attacks	*Phenotyping*
Chemical Combinatorial Attack	*Reverse Public Key Encryption*
Cryptophthora	*Standard Model*
Generic Model	*Temperature Attacks*
Groebner Basis	*Twin Signatures*
Monotone Signatures	*Von Neumann Correction*

Publications in 2010

149. Aurélie Bauer, Jean-Sébastien Coron, David Naccache, Mehdi Tibouchi, Damien Vergnaud: *On the Broadcast and Validity-Checking Security of PKCS#1 v1.5 Encryption*. ACNS 2010: 1-18 and IACR Cryptology ePrint Archive 2010: 135 (2010)

150. Benoît Chevallier-Mames, Jean-Sébastien Coron, Noel McCullagh, David Naccache, Michael Scott: *Secure Delegation of Elliptic-Curve Pairing*. CARDIS 2010: 24-35 and IACR Cryptology ePrint Archive 2005: 150 (2005)

151. Michel Agoyan, Jean-Max Dutertre, David Naccache, Bruno Robisson, Assia Tria: *When Clocks Fail: On Critical Paths and Clock Faults*. CARDIS 2010: 182-193

152. Michel Agoyan, Jean-Max Dutertre, Amir-Pasha Mirbaha, David Naccache, Anne-Lise Ribotta, Assia Tria: *How to flip a bit?* IOLTS 2010: 235-239

153. Marc Joye, David Naccache, Stéphanie Porte: *The Polynomial Composition Problem in (Z/nZ)[X]*. CARDIS 2010: 1-12 and IACR Cryptology ePrint Archive 2004: 224 (2004)

154. Georg Fuchsbauer, Jonathan Katz, David Naccache: *Efficient Rational Secret Sharing in Standard Communication Networks*. TCC 2010: 419-436 and IACR Cryptology ePrint Archive 2008: 488 (2008)

155. Jean-Sébastien Coron, David Naccache, Mehdi Tibouchi: *Fault Attacks Against EMV Signatures*. CT-RSA 2010: 208-220 and IACR Cryptology ePrint Archive 2009: 503 (2009)

156. Ahmad-Reza Sadeghi, David Naccache (Eds.): *Towards Hardware-Intrinsic Security - Foundations and Practice. Information Security and Cryptography*, Springer 2010, ISBN 978-3-642-14451-6

157. Yoo-Jin Baek, Vanessa Gratzer, Sung-Hyun Kim, David Naccache: Extracting Unknown Keys from Unknown Algorithms Encrypting Unknown Fixed Messages and Returning No Results. Towards Hardware-Intrinsic Security 2010: 189-197

158. Vanessa Gratzer, David Naccache: *How to Read a Signature?* Cryptography and Security 2012: 480-483 and IACR Cryptology ePrint Archive 2010: 530 (2010)

159. David Naccache, Igor Shparlinski: Divisibility, Smoothness and Cryptographic Applications. Algebraic Aspects of Digital Communications 2009: 115-173 and CoRR abs/0810.2067 (2008) and IACR Cryptology ePrint Archive 2008: 437 (2008)

Publications in 2009

160. Julien Brouchier, Tom Kean, Carol Marsh, David Naccache: Temperature Attacks. IEEE Security & Privacy 7(2): 79-82 (2009). Thermocommunication. IACR Cryptology ePrint Archive 2009: 2 (2009)

161. Mohaned Kafi, Sylvain Guilley, Sandra Marcello, David Naccache: *Deconvolving Protected Signals*. ARES 2009: 687-694

162. David Naccache, Rainer Steinwandt, Moti Yung: *Reverse Public Key Encryption*. BIOSIG 2009: 155-169

163. Jean-Sébastien Coron, Antoine Joux, Ilya Kizhvatov, David Naccache, Pascal Paillier: *Fault Attacks on RSA Signatures with Partially Unknown Messages*. CHES 2009: 444-456 and IACR Cryptology ePrint Archive 2009: 309 (2009)

164. Eric Brier, David Naccache, Mehdi Tibouchi: *Factoring Unbalanced Moduli with Known Bits*. ICISC 2009: 65-72 and IACR Cryptology ePrint Archive 2009: 323 (2009)

165. Julien Cathalo, David Naccache, Jean-Jacques Quisquater: *Comparing with RSA*. IMA Int. Conf. 2009: 326-335. IACR Cryptology ePrint Archive 2009: 21 (2009)

166. Antoine Joux, Reynald Lercier, David Naccache, Emmanuel Thomé: *Oracle-Assisted Static Diffie-Hellman Is Easier Than Discrete Logarithms*. IMA Int. Conf. 2009: 351-367 IACR Cryptology ePrint Archive 2008: 217 (2008)

Publications in 2008

167. Éric Levieil, David Naccache: Cryptographic Test Correction. IEEE Security & Privacy 6(2): 69-71 (2008). Public Key Cryptography 2008: 85-100

168. Don Coppersmith, Jean-Sébastien Coron, François Grieu, Shai Halevi, Charanjit S. Jutla, David Naccache, Julien P. Stern: Cryptanalysis of ISO/IEC 9796-1. J. Cryptology 21(1): 27-51 (2008) same result also appeared at Jean-Sébastien Coron, David Naccache, Julien P. Stern: *On the Security of RSA Padding*. CRYPTO 1999: 1-18 Robert Silverman, David Naccache *Recent results on signature forgery*, RSA Laboratories Bulletin, 11, April 1999, David Naccache, *Security of digital signature standards: The state of the art*, In S.-P. Shieh, Ed., 2nd International Workshop for Asian Public Key Infrastructures, pp. 159-163, Taipei, Taiwan, October 30-November 1, 2002 David Naccache: *Padding attacks on RSA*. Inf. Sec. Techn. Report 4(4): 28-33 (1999)

169. Benoît Chevallier-Mames, David Naccache, Jacques Stern: *Linear Bandwidth Naccache-Stern Encryption*. SCN 2008: 327-339 and IACR Cryptology ePrint Archive 2008: 119 (2008)

Publications in 2007

170. Vanessa Gratzer, David Naccache: Alien vs. Quine, the Vanishing Circuit and Other Tales from the Industry's Crypt. EUROCRYPT 2006: 48-58 and IEEE Security & Privacy 5(2): 26-31 (2007)

171. Vanessa Gratzer, David Naccache: Trust on a Nationwide Scale. IEEE Security & Privacy 5(5): 69-71 (2007)

172. David Naccache: Secure and Practical Identity-Based Encryption. CoRR abs/cs/0510042 (2005) and IACR Cryptology ePrint Archive 2005: 369 (2005) IET Information Security 1(2): 59-64 (2007)

173. Antoine Joux, David Naccache, Emmanuel Thomé: *When e-th Roots Become Easier Than Factoring*. ASIACRYPT 2007: 13-28 and IACR Cryptology ePrint Archive 2007: 424 (2007)

Publications in 2006

174. Jean-Sébastien Coron, David Naccache, Yvo Desmedt, Andrew M. Odlyzko, Julien P. Stern: Index Calculation Attacks on RSA Signature and Encryption. Des. Codes Cryptography 38(1): 41-53 (2006)

175. Hagai Bar-El, Hamid Choukri, David Naccache, Michael Tunstall, Claire Whelan: The Sorcerer's Apprentice Guide to Fault Attacks. Actes de DSN'04, Workshop on Fault Diagnosis and Tolerance in Cryptography, Florence, Italy, 30 June 2004. Pages 330-342. Cryptology ePrint Archive, Report 2004/100. How to explain fault attacks to your kids, by David Naccache In U. Schulte, Ed., ISSE 2002, on CD-ROM, Paris, France, October 2-4, 2002 and IACR Cryptology ePrint Archive 2004: 100 (2004). Proceedings of the IEEE, Volume:94, Issue: 2, pp. 370 - 382, 2006

176. Vanessa Gratzer, David Naccache: Cryptography, Law Enforcement, and Mobile Communications. IEEE Security & Privacy 4(6): 67-70 (2006). David Naccache: National Security, Forensics and Mobile Communications. ICISC 2005: 1. Vanessa Gratzer, David Naccache, David Znaty: Law Enforcement, Forensics and Mobile Communications. PerCom Workshops 2006: 256-260

177. David Naccache, Michael Tunstall, Claire Whelan *Computational Improvements to Differential Side Channel Attacks*, NATO Security through Science Series D: Information and Communication Security, vol. 2, IOS Press, pp. 26–35, 2006

Publications in 2005

178. Peter Gutmann, David Naccache, Charles C. Palmer: When Hashes Collide. IEEE Security & Privacy 3(3): 68-71 (2005)

179. David Naccache: Finding Faults. IEEE Security & Privacy 3(5): 61-65 (2005)

180. Vanessa Gratzer, David Naccache: *Blind Attacks on Engineering Samples*. IACR Cryptology ePrint Archive 2005: 468 (2005)

181. David Naccache, Phong Q. Nguyen, Michael Tunstall, Claire Whelan: *Experimenting with Faults, Lattices and the DSA*. Public Key Cryptography 2005: 16-28 and IACR Cryptology ePrint Archive 2004: 277 (2004)

182. Julien Cathalo, Jean-Sébastien Coron, David Naccache: *From Fixed-Length to Arbitrary-Length RSA Encoding Schemes Revisited*. Public Key Cryptography 2005: 234-243

Publications in 2004

183. Jean-Sébastien Coron, Paul C. Kocher, David Naccache: Statistics and Secret Leakage. Financial Cryptography 2000: 157-173 and ACM Trans. Embedded Comput. Syst. 3(3): 492-508 (2004)

184. Olivier Benoît, Nora Dabbous, Laurent Gauteron, Pierre Girard, Helena Handschuh, David Naccache, Stéphane Socié, Claire Whelan: *Mobile Terminal Security*. IACR Cryptology ePrint Archive 2004: 158 (2004). Appeared as a chapter in the book Network Security: Current status and Future Directions edited by Christos Douligeris and Dimitrios Serpanos, IEEE Press.

185. David Naccache, Nigel P. Smart, Jacques Stern: *Projective Coordinates Leak*. EUROCRYPT 2004: 257-267 and IACR Cryptology ePrint Archive 2003: 191 (2003)

186. Benoît Chevallier-Mames, David Naccache, Pascal Paillier, David Pointcheval: *How to Disembed a Program?* CHES 2004: 441-454 and IACR Cryptology ePrint Archive 2004: 138 (2004)

187. Claude Barral, Jean-Sébastien Coron, David Naccache: *Externalized Fingerprint Matching*. ICBA 2004: 309-315 and IACR Cryptology ePrint Archive 2004: 21 (2004)

188. Eric Brier, David Naccache, Pascal Paillier: *Chemical Combinatorial Attacks on Keyboards*. IACR Cryptology ePrint Archive 2003: 217 (2003) and *Chemické Komibinatorické Útoky na Klávesnice*, 5th Information Security Summit 2004, May 26-27, 2004, Prague, Tates International SRO (ISBN 80-86813-00-2), pp. 124--140.

189. Jean-Sébastien Coron, David Naccache: *Cryptanalysis of a Zero-Knowledge Identification Protocol of Eurocrypt '95*. CT-RSA 2004: 157-162

190. David Naccache, *Sécurité, cryptographie: théorie et pratique*, Mémoire d'habilitation à diriger des recherches, Université Paris VI et École normale supérieure, Paris, France, Décembre 2004

191. D. M'Raihi, J. Rydell, S. Machani, D. Naccache, S. Bajaj, *OCRA: OATH Challenge-Response Algorithms*, www.ietf.org/staging/draft-mraihi-mutual-oath-hotp-variants-13.txt and *HOTP: An HMAC-based One Time Password Algorithm*, « Internet Draft » IETF draft October 17, 2004 (draft-ietf-oath-hmac-otp-00.txt), David M'Raïhi, Mihir Bellare, Frank Hoornaert, David Naccache, Ohad Ranen.

Publications in 2003

192. Jean-Sébastien Coron, David Naccache: *Boneh et al.'s k-Element Aggregate Extraction Assumption Is Equivalent to the Diffie-Hellman Assumption*. ASIACRYPT 2003: 392-397

193. Konstantin Hyppönen, David Naccache, Elena Trichina, Alexei Tchoulkine: *Trading-Off Type-Inference Memory Complexity against Communication*. ICICS 2003: 60-71 and IACR Cryptology ePrint Archive 2003: 140 (2003)

194. David Naccache: Double-Speed Safe Prime Generation. IACR Cryptology ePrint Archive 2003: 175 (2003)

Publications in 2002

195. Helena Handschuh, David Naccache, Pascal Paillier, Christophe Tymen: *Provably Secure Chipcard Personalization, or, How to Fool Malicious Insiders*. CARDIS 2002

196. Jean-Sébastien Coron, Marc Joye, David Naccache, Pascal Paillier: *Universal Padding Schemes for RSA*. CRYPTO 2002: 226-241 and IACR Cryptology ePrint Archive 2002: 115 (2002)

197. David Naccache, Alexei Tchoulkine, Christophe Tymen, Elena Trichina: *Reducing the Memory Complexity of Type-Inference Algorithms*. ICICS 2002: 109-121 and Eurosmart 2002, French Riviera, France, September 19-20, 2002.

198. Nathalie Feyt, Marc Joye, David Naccache, Pascal Paillier, *Off-line/on-line generation of RSA keys with smart cards*, S.-P. Shieh, Ed., 2nd International Workshop for Asian Public Key Infrastructures, pp. 153-158, Taipei, Taiwan, October 30-November 1, 2002

199. Serge Lefranc, David Naccache: *Cut-&-Paste Attacks with Java*. ICISC 2002: 1-15. IACR Cryptology ePrint Archive 2002: 10 (2002)

200. Nils Maltesson, David Naccache, Elena Trichina, Christophe Tymen: *Applet Verification Strategies for RAM-Constrained Devices*. ICISC 2002: 118-137

Publications in 2001

201. David Naccache, David Pointcheval, Jacques Stern: *Twin signatures: an alternative to the hash-and-sign paradigm*. ACM Conference on Computer and Communications Security 2001: 20-27

202. Eric Brier, Christophe Clavier, Jean-Sébastien Coron, David Naccache: *Cryptanalysis of RSA Signatures with Fixed-Pattern Padding*. CRYPTO 2001: 433-439

203. David Naccache, David Pointcheval, Christophe Tymen: *Monotone Signatures*. Financial Cryptography 2001: 295-308

Publications in 2000

204. Jean-Sébastien Coron, François Koeune, David Naccache: *From Fixed-Length to Arbitrary-Length RSA Padding Schemes*. ASIACRYPT 2000: 90-96

205. David Naccache, Michael Tunstall: *How to Explain Side-Channel Leakage to Your Kids*. CHES 2000: 229-230

206. Jean-Sébastien Coron, David Naccache: *Security Analysis of the Gennaro-Halevi-Rabin Signature Scheme*. EUROCRYPT 2000: 91-101

207. Jean-Sébastien Coron, Marc Joye, David Naccache, Pascal Paillier: *New Attacks on PKCS#1 v1.5 Encryption*. EUROCRYPT 2000: 369-381

208. David Naccache, Jacques Stern: *Signing on a Postcard*. Financial Cryptography 2000: 121-135

209. Helena Handschuh, David Naccache, *SHACAL*, B. Preneel, Ed., First Open NESSIE Workshop, Leuven, Belgium, November 13-14, 2000

210. David M'Raïhi, David Naccache, Michael Tunstall: *Asymmetric Currency Rounding*. Financial Cryptography 2000: 192-201

Publications in 1999

211. Jean-Sébastien Coron, David Naccache, Pascal Paillier, Accelerating Okamoto-Uchiyama's public-key cryptosystem, par Electronics Letters, 35(4):291-292, 1999

212. Jean-Sébastien Coron, Helena Handschuh, David Naccache: *ECC: Do We Need to Count?* ASIACRYPT 1999: 122-134

213. David Naccache, Adi Shamir, Julien P. Stern: *How to Copyright a Function?* Public Key Cryptography 1999: 188-196

214. Jean-Sébastien Coron, David Naccache: *On the Security of RSA Screening*. Public Key Cryptography 1999: 197-203

Publications in 1998

215. David Naccache, Jacques Stern: *A New Public Key Cryptosystem Based on Higher Residues*. ACM Conference on Computer and Communications Security 1998: 59-66

216. Gérard D. Cohen, Antoine Lobstein, David Naccache, Gilles Zémor: *How to Improve an Exponentiation Black-Box*. EUROCRYPT 1998: 211-220

217. Jean-Sébastien Coron, David Naccache: *An Accurate Evaluation of Maurer's Universal Test*. Selected Areas in Cryptography 1998: 57-71

218. David M'Raïhi, David Naccache, David Pointcheval, Serge Vaudenay: *Computational Alternatives to Random Number Generators*. Selected Areas in Cryptography 1998: 72-80

Publications in 1997

219. David M'Raïhi, David Naccache, Jacques Stern, Serge Vaudenay: XMX: A Firmware-Oriented Block Cipher Based on Modular Multiplications. FSE 1997: 166-171

220. David Naccache, Jacques Stern: A New Public-Key Cryptosystem. EUROCRYPT 1997: 27-36

Publications in 1996

221. Markus Michels, David Naccache, Holger Petersen: GOST 34.10 - A brief overview of Russia's DSA. Computers & Security 15(8): 725-732 (1996)

222. David Naccache, David M'Raïhi: Cryptographic smart-cards, IEEE Micro, 16(3):14-24, 1996. Arithmetic co-processors for public-key cryptography: The state of the art. CARDIS 1996. Coprocessori aritmetici per crittografia a chiave pubblica, Fondazione Ugo Bordoni Conference (Rome), September 11-12, 1996. Japanese version in Nikkei Electronics, no. 672, pp. 95-110.

223. David M'Raïhi, David Naccache: *Batch Exponentiation: A Fast DLP-Based Signature Generation Strategy*. ACM Conference on Computer and Communications Security 1996: 58-61

Publications in 1995

224. David Naccache: A Montgomery-Suitable Fiat-Shamir-like Authentication Scheme. EUROCRYPT 1992: 488-491. David Naccache, David M'Raïhi, Dan Raphaeli: Can Montgomery Parasites Be Avoided? A Design Methodology Based on Key and Cryptosystem Modifications. Des. Codes Cryptography 5(1): 73-80 (1995). David Naccache, David M'Raïhi: Montgomery-Suitable Cryptosystems. Algebraic Coding 1993: 75-81

225. David Naccache, Signatures numériques et preuves à divulgation nulle, cryptanalyse, défense et outils algorithmiques, Thèse de doctorat, École Nationale Supérieure des Télécommunications, Paris, France, Mai 1995

226. David Naccache, David M'Raïhi, William Wolfowicz, Adina di Porto: *Are Crypto-Accelerators Really Inevitable? 20 Bit Zero-Knowledge in Less than a Second on Simple 8-bit Microcontrollers*. EUROCRYPT 1995: 404-409

Publications in 1994

227. Boo Barkee, Deh Cac Can (Deh Cac Can = D Naccache written backwards), Julia Ecks, Theo Moriarty, R. F. Ree: Why You Cannot Even Hope to use Gröbner Bases in Public Key Cryptography: An Open Letter to a Scientist Who Failed and a Challenge to Those Who Have Not Yet Failed. J. Symb. Comput. 18(6): 497-501 (1994)

228. David Naccache, *Colourful cryptography*, French Israeli Workshop on Coding and Information Theory, Ministry of science and the arts - Ministère des affaires étrangères, December 8, 1994

229. David Naccache, David M'Raïhi, Serge Vaudenay, Dan Raphaeli: *Can D.S.A. be Improved? Complexity Trade-Offs with the Digital Signature Standard*. EUROCRYPT 1994: 77-85 David M'Raïhi, David Naccache *Couponing scheme reduces computational power requirements for DSS signatures*, CardTech/SecurTech, pp. 99-104, Rockville, MD, USA, 1994, CTST Inc.

Publications in 1993

230. David Naccache: *Can O.S.S. be Repaired? Proposal for a New Practical Signature Scheme*. EUROCRYPT 1993: 233-239

231. David Naccache, *Unless modified Fiat-Shamir is insecure*, Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography: SPRC'93, Fondazione Ugo Bordoni, Ed. William Wolfowicz, Rome, Italy, pp. 172-180, 1993.

Publications in 1992

232. Sebastiaan H. von Solms, David Naccache: On blind signatures and perfect crimes. Computers & Security 11(6): 581-583 (1992)

233. Benjamin Arazi David Naccache, Binary-to-decimal conversion based on the divisibility of 255 by 5, Electronics Letters, vol 28. no. 23, 1992.

Publications in 1991

234. David Naccache, Michael Donio Accelerating Wilson's primality test, Revue Technique de Thomson CSF, vol. 23, no. 3, pp. 595-599, 1991.

Publications in 1990

235. David Naccache, Halim M'silti, A new modulo computation algorithm, Recherche Opérationelle – Operations Research (RAIRO-OR), vol. 24, no. 3, pp. 307-313, 1990.

236. David Naccache, A note about $\Sigma k^m k!$, The Pentagon, vol. 49, no.2, pp. 10-15, 1990.

237. David Naccache, On the generation of permutations, The South-African Computer Journal - Suid Afrikaanse Rekenaar-tydskrif, no. 2, pp. 12-15, 1990.

Publications in 1989

238. David Naccache, *Proposal for a recurrent enumeration of all the permutations on any set of mutually disjoint elements*, Scientific program and abstracts of the joint French-Israeli binational symposium on Combinatorics & Algorithms, Ministry of Science and Development - National Council for Research and Development, November 14-17, 1989.

Edited Proceedings

239. Luca Breveglieri, Sylvain Guilley, Israel Koren, David Naccache, Junko Takahashi (Eds.): *2011 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2011*, Tokyo, Japan, September 29, 2011. IEEE 2011, ISBN 978-1-4577-1463-4

240. Luca Breveglieri, Marc Joye, Israel Koren, David Naccache, Ingrid Verbauwhede (Eds.): *2010 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2010*, Santa Barbara, California, USA, 21 August 2010. IEEE Computer Society 2010, ISBN 978-0-7695-4169-3

241. Luca Breveglieri, Israel Koren, David Naccache, Elisabeth Oswald, Jean-Pierre Seifert (Eds.): *Sixth International Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2009*, Lausanne, Switzerland, 6 September 2009. IEEE Computer Society 2009, ISBN 978-0-7695-3824-2

242. Luca Breveglieri, Shay Gueron, Israel Koren, David Naccache, Jean-Pierre Seifert (Eds.): *Fifth International Workshop on Fault Diagnosis and Tolerance in Cryptography, 2008, FDTC 2008*, Washington, DC, USA, 10 August 2008. IEEE Computer Society 2008, ISBN 978-0-7695-3314-8

243. Luca Breveglieri, Shay Gueron, Israel Koren, David Naccache, Jean-Pierre Seifert (Eds.): *Fourth International Workshop on Fault Diagnosis and Tolerance in Cryptography, 2007, FDTC 2007*: Vienna, Austria, 10 September 2007. IEEE Computer Society 2007, ISBN 0-7695-2982-8

244. Luca Breveglieri, Israel Koren, David Naccache, Jean-Pierre Seifert (Eds.): *Fault Diagnosis and Tolerance in Cryptography, Third International Workshop, FDTC 2006*, Yokohama, Japan, October 10, 2006, Proceedings. Lecture Notes in Computer Science 4236, Springer 2006, ISBN 3-540-46250-3

245. David Naccache, Pascal Paillier (Eds.): *Public Key Cryptography, 5th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2002*, Paris, France, February 12-14, 2002, Proceedings. Lecture Notes in Computer Science 2274, Springer 2002, ISBN 3-540-43168-3

246. Çetin Kaya Koç, David Naccache, Christof Paar (Eds.): *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop*, Paris, France, May 14-16, 2001, Proceedings. Lecture Notes in Computer Science 2162, Springer 2001, ISBN 3-540-42521-7

247. David Naccache (Ed.): *Topics in Cryptology - CT-RSA 2001, The Cryptographer's Track at RSA Conference 2001*, San Francisco, CA, USA, April 8-12, 2001, Proceedings. Lecture Notes in Computer Science 2020, Springer 2001, ISBN 3-540-41898-9

248. David Naccache, Damien Sauveron: *Information Security Theory and Practice. Securing the Internet of Things - 8th IFIP WG 11.2 International Workshop, WISTP 2014*, Proceedings. Lecture Notes in Computer Science 8501, Springer 2014, ISBN 978-3-662-43825-1

249. Ion Bica, David Naccache, Emil Simion: *Innovative Security Solutions for Information Technology and Communications - 8th International Conference, SECITC 2015*, Bucharest, Romania, June 11-12, 2015. Revised Selected Papers. Lecture Notes in Computer Science 9522, Springer 2015, ISBN 978-3-319-27178-1

250. Michael Reiter, David Naccache: *Cryptology and Network Security - 14th International Conference, CANS 2015*, Marrakesh, Morocco, December 10-12, 2015, Proceedings. Lecture Notes in Computer Science 9476, Springer 2015, ISBN 978-3-319-26822-4

251. David Naccache, Shouhuai Xu, Sihan Qing, Pierangela Samarati, Gregory Blanc, Rongxing Lu, Zonghua Zhang, Ahmed Meddahi: Information and Communications Security - 20th International Conference, ICICS 2018, Lille, France, October 29-31, 2018, Proceedings. Lecture Notes in Computer Science 11149, Springer 2018, ISBN 978-3-030-01949-5

Examples of press reports on my works (partial illustrative list)

- L'Usine Nouvelle « Les 100 de la Cyber Sécurité 2018 : David Naccache arme les industriels »
- 2017-2019 : Long interviews in 5 episodes of the documentary series « Non élucidé » (« Unsolved Case ») and « Indices » (« Clues ») shot by the production company Phare Ouest. I commented on murder cases where my GSM and GPS forensic expertise was useful. Those episodes deal with the murders of victims Nathalie Villermet, Nicole Saada, Stéphane Kameugne (murder or accident), Jennifer Charron and Michèle Laforge.
- Le Monde : « *Des Cryptologues Déchiffrent un Terme Censuré Dans un « Mémo » Adressé par la CIA à George Bush* ».
- The New York Times : « *Researchers Develop Techniques To Being Blacked-Out Words To Light* ».
- Nature : « *US Intelligence Exposed as Student Decodes Iraq Memo* ».
- The International Herald Tribune : « *Censoring: You Can Write But Can't Hide* ».
- Facts : « *Nachhilfe für die CIA* »
- The Irish Times : « *Code Cracker Triumphs in Battle of Wits* »
- The Washington Post : « *Disappearing Ink* ».
- Oaklabd Tribune, San Mateo County Times, Tri Valley Herald et Alameda Times Star : « *Computers Can Show Blacked-Out Words* »
- NRC Handelsblad : « *Informatici ontcijferen geheime documenten* »
- Der Spiegel : « *Informatiker knacken zensierte Geheimdokumente* »
- Heise Online : « *Kryptologen enthüllen Regierungsgeheimnisse* »

Responsible disclosure (An example: Critical security flaw in Microsoft's cloud service)

https://www.microsoft.com/en-us/msrc/researcher-acknowledgments-online-services-archive?rtc=1

PATENTS (PARTIAL LIST)

David Naccache

- Each entry is a patent family (different inventive idea).
- I am France's most prolific living inventor (http://tinyurl.com/Naccache5, p. 23; 8 inventors filed >110 patents).
- As of 01/10/2022, nine more patent ideas are under examination (not published yet hence absent in this list).

1. Marc Beunardeau, Aisling Connolly, Rémi Géraud, David Naccache, Elena Trichina, Système et procédé d'authentification et de signature numérique, FR20170057933 FR3070517

2. Hsiao-Ying Lin, Tieyan Li, David Naccache, Yanjiang Yang, Mingming Zhang, Xiaopeng Zhao, Method and apparatus for updating devices in a remote network. WO2019182509 US2021004221

3. Beunardeau Marc, Géraud Rémi, Connolly Aisling, Naccache David, Procédé de réduction de la taille d'une base de données répartie de type chaîne de blocs, dispositif et programme correspondant, FR3062499

4. Beunardeau Marc, Géraud Rémi, Naccache David, Connolly Aisling, Encryption method, decryption method, device and corresponding computer program, FR3057374 WO2018069465 CA3039737 EP3526946 US11075756

5. Naccache David, Géraud Rémi, Device, method and program for securely reducing an amount of record in a database EP3321819 US2018129700 CA2984833 ES2819888

6. Naccache David, Quaglia Elizabeth, Smyth Benjamin, System and method for efficient and secure communication between devices, WO2018143895 SG10201700811V US11228589

7. Naccache David, Géraud Rémi, Quentin Pierre, Ducrohet Vincent, Delord Christian, Method for processing data on a multimedia payment kiosk, corresponding devices and computer programs CA3003508 EP3369067 FR3042933 WO2017072056 US2018308080 ES2841905

8. David Naccache, Lukasz Jeczminski, Mateusz Zajakala, Jas Saini, Process for reinforcing the security of a pay television system based on periodic mandatory back communication. CN107547946 PL3264306 EP20170172165

9. Naccache David, Quentin Pierre, Procédé de détection d'un risque de substitution d'un terminal, dispositif, programme et support d'enregistrement correspondants CA2960914 CA20152960914 FR20140058749 WO2015EP71129 US10650381

10. Naccache David, Mayer Laurent, Method of auto-detection of an attempted piracy of an electronic payment card, corresponding card, terminal and program CA2961274 CA20152961274 FR20140059134 WO2015EP71955 US2017278109 PL3198540

11. Naccache David, Ardila German, Method for wireless transmission of data to a magnetic reading head, communication terminal and corresponding program WO2016110591 WO2016EP50319 FR20150050190 US10187119

12. Naccache David, Géraud Rémi, Léger Michel, Device and method for securing commands exchanged between a terminal and an integrated circuit CA2940465 CA20162940465 FR20150057983 ES2848284

13. Naccache David, Jean-Louis Sarradin, Method for checking the authenticity of a payment terminal and terminal thus secured BR102015031467 BR20151031467 FR20140062139 ES2786267

14. Géraud Rémi, Koudoussi Hiba, Naccache David, Securing a confirmation of a sequence of characters, corresponding method, device and computer program product US2017004330 US201615201549 CA2934715 EP3113056 ES2721275 FR3038422 PL3113056

15. Naccache David, Géraud Rémi, Koudoussi Hiba Method for securing at least one memory zone of an electronic device, and corresponding security module, electronic device and computer program WO2017102663 WO2016EP80684 FR20150062428 CA3007450 US2018373624 ES2763818

16. Naccache David, Géraud Rémi, Beunardeau Marc, Method for transmitting data, method for receiving data, corresponding devices and programs US2017187692, US201615388411, FR20150063338

17. Naccache David, Géraud Rémi, Koudoussi Hiba Data encryption process for methods of payment, corresponding methods of payment, server and programs CA2947920 CA20162947920 FR20150060772 ES2901148

18. David Naccache, Method for authenticating a user, corresponding server, communication terminal and programs. BR20151031254 EP3032799 US2016173473 FR3030083 CA2914426 ES2699925 PL3032799

19. David Naccache, Method, sender apparatus and receiver apparatus for modulo operation. US5479511 SG44714 HK1000987 ES2101124 EP0611506 EP0611506 DE69218961 AU2883692 WO9309620.

20. David Naccache, Apparatus and method for modulo computation. EP0515956 ZA9203803 TR26124 MX9202480 WO9222028 CN1070298 AU1764192

21. David Naccache, Patrice Fremanteau, Unforgeable identification device, identification device reader and method of identification. US5434917 EP0583709 CN1032940 CN1082742

22. David Naccache, Method, identification device and verification device for identification and/or performing digital signature. US5502764 JPH06505343 JP3456993 EP0570388 EP0502559 DE69202699 CA2101322 AU1159292 AU648643 WO9214318

23. David Naccache, Method for executing number-theoretic cryptographic and/or error-correcting protocols. EP0578059 ES2203612 DE69333121

24. David Naccache, Method for performing public-key cryptography. EP0577000 DE69320715

25. David Naccache, Method and apparatus for access control and/or identification WO9213321 PL168163 JPH06504626 JP3145116 HK135597 EP0567474 EP0496459 DE69206126 CA2100576 AU1157992 AU650321 US5452357

26. David Naccache, Eric Diehl, Apparatus and method for access control SG46722 JPH06197341 JP3665352 HK1009313 ES2105021 DE69312828 AU4615693 AU667231 US5461675

27. David Naccache, Eric Diehl, Method for access control. EP0588184

28. David Naccache, Patrice Fremanteau, Wolfgang Hartnack, Method and apparatus for controlling and/or limiting speed excess by drivers, Method and apparatus for controlling speed excess of a moving object. EP0588049 US5654891 DE69323135

29. David Naccache, Method and apparatus for modulo computation. CN1079349 AU3890093 WO9320503

30. David Naccache, Etienne Cochon, Michel Poivet, Albert Dörner, Adrian Robinson, Christopher Clarke, Andrew Bower, Method and apparatus for secure transmission of video signals. WO9307718 TR26360 TR26199 TR27057 TR27727 MX9205588 MX9205587 JPH06511124 JPH06511123 JPH06511122 WO9307717 EP0606346 EP0606328 EP0606328 EP0606300 EP0606300 WO9307716 CN1071797 CN1071039 CN1074072 AU2678392 AU2657092 AU2646892 US5555305 WO9307718 MY108367 ZA927511

31. David Naccache, Patrice Fremanteau, Wolfgang Hartnack, Card, card reader and method for protocol selection. EP0583723 SG48324 EP0583526

32. David Naccache, David M'Raïhi, System for improving the digital signature algorithm. US5414772

33. David Naccache, David M'Raïhi, Verification process for a communication system. JPH07312592 ES2148296 EP0643513 EP0643513 DE69424729 US5347581

34. David Naccache, David M'Raïhi, Process for generating DSA signatures with low-cost portable apparatuses. EP0656710 US5625695 FR2713419 ES2263148 DE69434703 FR2713420

35. David Naccache, David M'Raïhi, Method for implementing a private key communication protocol between two processing devices. US6226382 JPH10511778 FR2728981 ES2132764 EP0800691 DE69509127 CA2208983 AU4451696 AT179009 WO9620461

36. David Naccache, David M'Raïhi, Jacques Stern, Serge Vaudenay, Method of cryptography with public key based on the discrete logarithm US5946397 JPH10500502 FR2739469 ES2279525 EP0795241 DE69636772 WO9713342

37. David Naccache, David M'Raïhi, Public key cryptography method. WO9747110 US6459791 JP2000511649 ES2227595 EP0909495 DE69633253 CA2257907 FR2734679

38. David Naccache, David M'Raïhi, Process for generating electronic signatures, in particular for smart cards. US5910989 JPH10506727 JP3433258 FR2733379 EP0766894 WO9633567

39. David Naccache, David M'Raïhi, Procédé de signature numérique de messages. FR2733378

40. Jacques Stern, Françoise Lévy-dit-Vehel, David Naccache, Method for signing and/or authenticating electronic messages. FR2756122 JP2001503162 WO9823061 EP0940021 CA2271989

41. David Naccache, Françoise Lévy-dit-Vehel, Jacques Stern, Système cryptographique comprenant un système de chiffrement et déchiffrement et un système de séquestre de clés, et les appareils et dispositifs associés. US2005123131 US20040817453; FR19970002244; US19980837662; US19990377666 FR2759806 JP2001503164 WO9837662 ES2216276 EP0962069 DE69821091 CN1248366 CA2280952

42. Françoise Lévy-dit-Vehel, David Naccache, David M'Raïhi, Pseudo-random generator based on a hash coding function for cryptographic systems requiring random drawing. FR2763194 JP2001507479 WO9851038 EP0980607 CN1262830 CA2288767 AU7659598

43. David Naccache, Nathalie Fëyt, Olivier Benoît, Device for hiding operations performed in a microprocessor card. US6698662 FR2776410 JP2002508549 ES2214012 EP1062633 DE69913667 CN1288548 CN1179298 CA2323006 WO9949416

44. David Naccache, Jean-Sébastien Coron, Method for testing a random number source and electronic devices comprising said method. WO0010284 FR2782401 US6990201 MXPA01001785 JP2002523815 EP1105997 CN1323477 AU5173299

45. David Naccache, Philippe Anguita, Electronic component for masking execution of instructions or data manipulation FR2784763 JP2002528784 EP1121629 CN1332860 AU6207799 WO0023866

46. David Naccache, Jean-Sébastien Coron, Nathalie Fëyt, Olivier Benoît, Method for countermeasure in an electronic component using a secret key algorithm, WO0049765 FR2789776 US7471791 MXPA01008201 JP2002540654 ES2262502 EP1198921 DE60027163 CN1630999 CN100393029 AU3057500

47. David Naccache, Pierre Girard, Ludovic Rousseau, Method for monitoring a program flow FR2790844 US7168065 MXPA01009056 JP2002539523 JP4172745 EP1161725 DE60001393 CN1350675 AU3058900 AT232616 WO0054155

48. David Naccache, Countermeasure method in an electronic component using a dynamic secret key cryptographic algorithm. US7206408 FR2793571 WO0068901 ES2287013 EP1180260 DE60034944 CN1360715 CN1231871 AU4415900

49. David Naccache, Jean-Sébastien Coron, Method for improving a random number generator to make it more resistant against attacks by current measuring. US7146006 FR2796477 WO0106350 EP1200889 CN1360692 AU6452700 AT226331

50. David Naccache, Jacques Stern, Jean-Sébastien Coron, Signature schemes based on discrete logarithm with partial or total message recovery. FR2797127 EP1205051 CN1377539 AU6575300 WO0110078

51. David Naccache, Pascal Paillier, Protection against abusive use of a statement in a storage unit. US2002174309 FR2814557 EP1325418 CN1392980 AU9200201 WO0227500

52. David Naccache, Nora Dabbous, Method for calculating cryptographic key check data. method for calculating a cryptographic key control datum US2003103625 FR2808145 EP1277306 CN1426645 AU5487701 WO0182525

53. David Naccache, Nora Dabbous, Procédé d'inscription d'une séquence de caractères et support comportant une inscription obtenue selon le procédé. FR2806660

54. David Naccache, Pascal Paillier, Jacques Stern, Procédé de signatures numériques probabilistes. FR2807248 WO0174009 US2001056537 EP1269683 AU4425901

55. David Naccache, Christophe Tymen, Method for cryptographic calculation comprising a modular exponentiation routine FR2810178 WO0197009 AU6402601

56. David Naccache, Christophe Bidan, Pierre Girard, Pascal Guterman, Ludovic Rousseau Contrôle d'accès à un moyen de traitement de données FR2810481 US2003188170 US8583934 WO0199064 ES2263635 EP1297501 DE60119111 CN1437739 CN1279497 AU6921801

57. David Naccache, Nora Dabbous, Countermeasure method in a microcircuit therefor and smart card comprising said microcircuit. FR2808360 WO0184491 US2004039931 US7809959 ES2312427 EP1279141 CN1426573 CN1218277 AU5487901 AT403911

58. David Naccache, Christophe Tymen, David Pointcheval, Multiple-level electronic signature method FR2817422 WO0245338 EP1344344 AU2201302

59. David Naccache, Jean-Sébastien Coron, A method for encoding long messages for electronic signature schemes based on RSA. FR2814619 WO0228010 US2003165238 EP1325584 CN1393081 AU9200301

60. David Naccache, Jean-Sébastien Coron, Method for accelerated transmission of electronic signature FR2814620 WO0228011 US2002188850 EP1325585 CN1393080 AU9200401

61. David Naccache, Serge Lefranc, Countermeasure method for improving security of transactions in a network FR2814306 WO0223313 AU9000401

62. David Naccache Method for protection against fraud in a network by icon selection FR2815204 US2003191967 US7340599 WO0231631 EP1327185 DE60131872 CN1468394 AU9000301 AT381066

63. David Naccache, Matthieu Vavassori, Method for managing computer applications by the operating by the operating system of a multi-application computer system. FR2819602 WO02056174

64. David Naccache, Christophe Tymen, Method for multiplying two binary numbers. US2004143618 FR2820851 WO02065271 EP1362284

65. David Naccache, Pascal Paillier, Helena Handschuh, Christophe Tymen, Identification module provided with a secure authentication code US2004153659 FR2820916 WO02065413 EP1362334 US2004153659

66. David Naccache, Frédéric Amiel, Procédé de contre mesure dans un composant électronique mettant en oeuvre un algorithme de cryptographie. FR2818846

67. David Naccache, David Pointcheval, Benoît Chevallier-Mames, Procédé et dispositif de vérification de données signées par groupe et application pour la transmission de données depuis une mémoire annexe. FR2831364

68. David Naccache, Marc Joye, Stéphanie Porte, Method and device for verifying possession of a confidential information without communicating same, based on a so-called zero knowledge process. FR2830147 WO03036865

69. David Naccache, David Pointcheval, Helena Handschuh, Cryptographic method using a data flow symmetrical cryptographic algorithm and use in a smart-card. FR2836311 WO03071735 EP1479189 AU2003222578

70. David Naccache, Jean-Sébastien Coron, Method of reducing the size of an RSA or Rabin signature. FR2829333 WO03021864 AU2002341079

71. David Naccache, Jean-Sébastien Coron, Procédé de vérification de codes pour microcircuits à ressources limitées. FR2832821

72. David Naccache, Marc Joye, Jean-Sébastien Coron, Pascal Paillier, Procédé de chiffrement de données, système cryptographique et composant associés. FR2842967 US2006147039 JP2005534068 WO2004012372 EP1535424 AU2003269063

73. David Naccache, Claude Barral, Jean-Sébastien Coron, Cedric Cardonnel, Procédé et dispositif d'identification biométrique adaptés à la vérification sur cartes à puce. US7433501 FR2855889 MXPA05013124 ES2353720 WO2004109585 EP1634220 AT484032

74. David Naccache, Procédé, support d'authentification, et dispositif perfectionnés pour la sécurisation d'un accès à un équipement. FR2867002 US2007168667 EP1726120 WO2005093993

75. David Naccache, Pascal Paillier, Benoît Chevallier-Mames, Procédé d'authentification dynamique de programmes par un objet portable électronique. FR2867929 WO2005101725 EP1728354

76. David Naccache, Jean-Sébastien Coron, Benoît Chevallier-Mames, Marc Chancerel, Procédé de réalisation d'une opération de couplage sur une courbe elliptique, par un système comprenant une carte à puce et un lecteur de carte. WO2005125085 FR2871970

77. Naccache David, Cardonnel Cédric, Rouchouze Bruno, Procédé et dispositif perfectionnés de ratification de données probatoires représentant un degré de ressemblance non nécessairement binaire avec une donnée de référence. WO2006061435

78. Brouchier Julien, Brier Eric; Naccache David, Dispositif de stockage de données sécurisé, WO2006128770 FR2886748

79. David Naccache, Jean-Sébastien Coron, Eric Brier, Cédric Cardonnel, Procédé de chiffrement de données numérique, procédé de masquage d'une empreinte biométrique, et application à la sécurisation d'un document de sécurité. US2007183636 US7895440 WO2005111915 FR2870413 EP1747526 DK1747526 AT541267

80. Naccache David, Procédé cryptographique mettant en œuvre un système de chiffrement basé sur l'identité. WO2007042419 FR2892251

81. Naccache David, Procédé de transmission d'un code confidentiel, terminal lecteur de cartes, serveur de gestion et produits programme d'ordinateur correspondants. FR2922395 EP2048632 US2009095809 CA2640945

82. Naccache David, Procédé d'authentification biométrique, programme d'ordinateur, serveur d'authentification, terminal et objet portatif correspondants. FR2922396 EP2048814 US2009100269 CA2640915 BRPI0804264

83. Naccache David, Terminal de paiement électronique, Procédé de vérification de conformité d'au moins une batterie amovible d'un tel terminal, batterie amovible et produit programme d'ordinateur correspondants. FR2928515 EP2099089 US2009230180 US8074888 ES2698225 PL2099089

84. Naccache David, Procédé de sécurisation d'un programme informatique, dispositif, procédé de mise à jour et serveur de mise à jour correspondants. FR2927436 EP2090984 US2009204952 ES2349908 AT475933

85. Naccache David, Dabbous Nora, Procédé de sécurisation d'un microprocesseur, programme d'ordinateur et dispositif correspondants, FR2925968 EP2079034 US2009172268 PT2079034 US2009172268 ES2391676 PL2079034

86. Naccache David, Procédé de gestion d'enchères électroniques, système et produit programme d'ordinateur correspondants. FR2925733.

87. Naccache David, Information processing device comprising a read-only memory and a method for patching the read-only memory, EP2523105 US2012290773 RU2012119211 JP2012238312

88. Naccache David, Coron Jean-Sébastien, Tibouchi Mehdi, Dispositif et procédé de compression de clés publiques pour algorithme de chiffrement pleinement homomorphique. FR2979043 WO2013024230

89. Naccache David, Coron Jean-Sébastien, Tibouchi Mehdi, Dispositif et procédé de génération de clés à sécurité renforcée pour algorithme de chiffrement pleinement homomorphique. FR2975248 WO2012152607 CA2832156 US2014233731 ES2546560

90. Naccache David, Procédé d'authentification biométrique, système d'authentification, programme et terminal correspondants. FR2922340 EP2048592 US2009097714 US8577090 ES2349359 CA2640856 BRPI0804241 AT475143.

91. Naccache David, Procédé de sécurisation et dispositif mobile ainsi sécurisé. FR2913296 US2008218347 EP1965328 HRP20150236 CA2913381

92. Naccache David, Circuit intégré, procédé de test, dispositif et programme d'ordinateur correspondants. FR2912551 EP1959266 US2008195345 US7966145

93. Naccache David, Module de sécurité matériel, procédé de mise en service et terminal de paiement électronique utilisant ce module. FR2910991 EP1944723 US2008163376 ES2330156

94. Naccache David, Procédé de lutte contre le vol de billets, billet, dispositif d'inactivation et dispositif d'activation correspondants. FR2907948 EP1916631 US2008100449 US7800502 AT518218

95. Naccache David, Alarm device comprising an electronic funds transfer at point of sale terminal and use thereof. US2008055107 EP1903527 FR2905503

96. Naccache David, Electronic payment terminal and method for making electronic payment terminals available. US2008046381 FR2905022 EP1912168

97. David Naccache, Method and device for authenticating a user. ES2792177 FR2902253 EP1868316 US2008077977 JP2007336546 CN101090322

98. Naccache David, Method for verifying conformity of the logical content of a computer appliance with a reference content. EP1830295 DE202006020631 ES2792173 WO2007099224. US2009260084 EP1830293

99. Naccache David, Electronic payment terminal e.g. computer, for e.g. storing secured payment transaction, has membrane keyboard with transparent mechanical keys that are defined in display zone, and display managing unit in connection with keyboard. FR2907927.

100. Naccache David, Touch screen for e.g. computer, has non-tactile display subjected to substantial local deformation, when local pressure is applied, and transducers arranged with respect to display, so that deformation stimulates one transducer. FR2907563

101. Naccache David, Terminal de paiement électronique biométrique et procédé de transaction. FR2905187, WO2008023114 US2010030696 EP2082364

102. Naccache David, Procédé de commande d'actions au moyen d'un écran tactile. FR2963970 WO2012022769 US2013201106 EP2606415 CA2807604 ES2862342

103. Naccache David, Brier Eric, Method and system for validating a transaction, and corresponding transactional terminal and programme. MX2011003136 EP2369780 US2011238513 US8380574 FR2958102 CN102201091 BRPI1100931 ES2701726 PL2369780

104. Naccache David, Brier Eric, Patrice Le Marre, Sarradin Jean-Louis, Coron Jean-Sebastien, Aubanel Jean-Marie, Method for reducing the power consumption of an electronic terminal, corresponding terminal and computer program. MX2011002307 EP2363781 US2011214000 FR2956912 CN102193618 BRPI1101809 ES2742327

105. Naccache David; André Guillaume; Hernandez Vincent; Delorme Jean-Jacques; Sarradin Jean-Louis; Bern Frédéric; Marsaud Thierry; Olive Jean-Louis, Dispositif de saisie de données en Braille, procédé et produit programme d'ordinateur correspondants. FR2965962 WO2012045844 EP2625682 CA2810318 US2013321302 BR112013006281 WO2011EP67514

106. Naccache David, Système et méthode permettant de diminuer l'encombrement sur un réseau de télécommunication mobile. FR2955227

107. Naccache David, Sabeg Karim, Dispositif et procédé de multiplication rapide. FR2974917 FR2974916 WO2012150396

108. Naccache David, Système et méthode permettant d'accélérer le choix dans une liste déroulante. FR2956760

109. Cioranesco Jean-Michel, Naccache David, Protection d'un circuit intégré contre des attaques invasives. EP2624296

110. Naccache David, Système et méthode permettant d'échanger communications et messages avec un usager de transports en commun via un réseau de télécommunications mobiles. FR2957474

111. Naccache David, Andre Guillaume, Hernandez Vincent, Delorme Jean-Jacques, Sarradin Jean-Louis, Bern Frederic, Marsaud Thierry, Olive Jean-Louis, Portable device including a touch screen and corresponding method for using same. WO2011141391 US2013135238 FR2960087 EP2569765 CN102939625 CA2797321

112. Naccache David, Method for assuring biometric authentication of user for allowing user to carry out e.g. payment, involves comparing authentication data with reference biometric data, and providing authentication assertion when two data are same. FR2958818

113. Naccache David, Method for biometric authentication, authentication system and corresponding program. FR2956942 WO2011101407 US2013040606 FR2956941 EP2537286 EA201201130 CA2787721 ES2477597 BR112012019749 WO2011EP52349

114. Naccache David, Polechtchouk Pavel, Display method, corresponding device and computer program product. US8495600 EP2219113 MX2010001687 FR2942056 CA2692588 BRPI1002208 ES2769273

115. Naccache David, Method for simplifying user input of a numerical sequence of large length, corresponding device and computer program product. EP2323063. US2011087995 FR2951289 BRPI1004008

116. Naccache David, Polechtchouk Pavel, Pointcheval David, Cryptographic message signature method having strengthened security, signature verification method, and corresponding devices and computer program products. US2011064216 EP2296308 FR2950212 CN102025502 BRPI1003364

117. Naccache David, Method for securing transactions, transaction device, bank server, mobile terminal, and corresponding computer programs. US2010198725 EP2199966 FR2940567

118. Naccache David, Method for assisting in the checking of transaction records, transaction device, server, mobile terminal, and corresponding computer programs. US2010185535 EP2207150 FR2940489

119. Naccache David, Traceability method for an electronic payment terminal in the event of a theft thereof, and corresponding computer program. US2009207021 US8106771 EP2091017 FR2927446

120. Naccache David, Dolique Christophe, Access control method, corresponding device and computer program product. US2009224872 EP2091025 FR2927452

121. Naccache David, Method for authenticating micro-processor cards, corresponding micro-processor card, card reader terminal and programs. US2009200372 US7971785 EP2091028 FR2927454 PL2091028

122. Naccache David, Terminal theft protection process, and corresponding system, terminal and computer program. US2009151010 US8182549 EP2068289 FR2924846

123. Naccache David, Method for manufacturing a portable payment terminal, corresponding terminal, device and battery. US2009095808 EP2048733 FR2922399

124. Naccache David, Authentication method, corresponding portable object and computer software program. US2009100240. EP2048631 FR2922394 CA2640916 BRPI0804240

125. Naccache David, Troumelin Michael, Payment terminal, associated method and program. EP1983480. US2008257954 US8074872 FR2915302

126. Naccache David, Hardware security module, commissioning method and electronic payment terminal using this module. US20080163376A1 FR2910991B1 DE602007001571D1

127. Naccache David, Method for auditing compliance of an electronic platform and/or a computer program present on said platform, and device and computer program corresponding thereto. US2008155507 US8171456 EP1942428 FR2910657

128. Naccache David, Method of providing transaction data, terminal, transaction method, method of enhancing bank statements, server, signals and computer program products corresponding thereto. US2008103912 US8219469 EP1916623 FR2907942

129. Naccache David, Method of printing receipts. US2010044425 FR2907577 FR2907576 US2010044425 US8556171 WO2008049998 EP2A084678 ES2547227

130. Naccache David, Polechtchouk Pavel, Méthode de traitement de données transactionnelles, terminal, serveur et programmes d'ordinateur correspondants, EP2884415 US2015161744 FR3014586 CA2872691 BR102014029693 MX2014014762

131. Achari Karim, Naccache David, Procédé de contrôle d'une identité d'un terminal de paiement et terminal ainsi sécurisé, FR3015077

132. David Naccache, Apparatus and method for forming secure computational resources, US201213488340 WO2013184567

133. David Naccache, Magnetic head for a payment terminal, WO2015110610 FR3016994 CA2937706 US2016350562 EP3097510 ES2715501 US9886602 PL3097510

134. David Naccache, Method of transmitting encrypted data, method of reception, devices and computer programs corresponding thereto, WO2015107175 FR3016762 CA2936584 = Method for transmitting encrypted data, method for receiving, corresponding devices and computer programs. US2016380980 US201515111069 FR20140050408 WO2015EP50823

135. David Naccache, Nora Dabbous, Device for processing data from a contactless smart card, method and corresponding computer program. WO2015158621 FR3020167 US2017039401 CA2945878 EP3132403 PL3132403 US10146966 ES2707504 WO2015EP57844

136. David Naccache, Laurent Mayer, Bilal El Kouche, Module for emulating at least one payment card, and processing method, payment device, computer program product and storage medium. FR3020164 WO2015158888 US2017185995 PL3132404 CA2945551 EP3132404 ES2725456

137. David Naccache, Alain Soubirane, Laurent Mayer, Nora Dabbous, Pierre Quentin, Method for verifying the authenticity of a terminal, corresponding device and program. EP2927857 US2015278792 FR3019357 CA2886164 BR102015007160

138. James Sébastien, Pierre Pignal, Sylvain Barneron, David Naccache, Method for managing the entry of data by pressing on a touch surface of an electronic terminal, and the corresponding module, terminal, computer program product and storage medium. EP2930606 FR3019916 CA2887619 US2015293662 BR102015007978 FR20140053195 ES2744330

139. David Naccache, Pierre Quentin, Eric Brier, Dorina Ghiliotto-Young, Method for deactivating a payment module, corresponding computer program product, storage medium and payment module. EP2933767 FR3020163 US2015302403 CA2887937 BR102015008606 ES2744269

140. David Naccache, Fabien Demange, Pierre Martinez, Code protector for electronic terminal keypad and corresponding electronic terminal, BR20151011881, EP2950284 US2015340177 FR3021423 CA2891697 BR102015011881 PL2950284 (T3), EP20150167408 FR20140054643

141. David Naccache, Wang Guilin, Quaglia Elizabeth, Method and system for symmetric swarm authentication, WO2018199847 SG10201703532P CN110945832

142. David Naccache, Guilin Wang, Method and Apparatus for Swarm Authentication of a Plurality of Proving Devices by Using Distributed Identification Schemes (Alternative title: Method and system for performing collective authentication in a communication network), Patent application No. SG10201700379U, No. SG10201600445T CN108337092

143. David Naccache, Rémi Géraud, Method for modulating access to a resource, corresponding program and device, FR3048529, US2017255787 ES2893173

144. David Naccache, Lukasz Jeczminski, Mateusz Zajakala, Jas Saini, Method and device allowing an access control system to be applied to the protection of streamed video, EP3236632 FR3050599 US2017311007 PL3236632

145. David Naccache, Polechtchouck Pavel, Elena Trichina, System and method for exchanging payment data between a cash register and a device for acquiring electronic payments. CA3143861, WO2020FR51078 FR1906851A

146. Thomas Souvignet, David Naccache, Thibaut Heckmann, Electrically conductive adhesive and (re)generation of (micro)electric circuits, WO2020084202 (A1), FR20180071296

147. Cheng Kang Chu, David Naccache, Jie Shi, Chengfang Fang, Xiwen Frang, Information processing method, terminal device, and network system, US2021135858.

148. Rémi Géraud, Hiba Koudoussi, David Naccache, Processing data update or data insertion request, FR3112631 WO2022013071

149. Michel Léger, David Naccache, Method for controlling the dispoaly of information on a screen of an electronic data-input device, corresponding device and computer program product, WO2021165104, CA3170644 FR3107373

150. David Naccache, Rémi Géraud, Marc Beunardeau, Data-transmission method, data-receiving method, corresponding devices and programs, ES2764127, FR3046274 US10491570,

151. David Naccache, Marc Beunardeau, Aisling Connolly, Rémi Géraud, Hiba Koudoussi, Transaction authentication method, server and system using two communication channels, WO2021116627 CA3161325 FR3104760

152. David Naccache, Michel Léger, Elena Trichina, Method and system, device and payment terminal using personal data, FR3104779 CA3161315 WO2021116625

Service des ressources humaines

Affaire suivie par : Yohann AUGER
Téléphone : 01.44.32.29.43
Mél : yohann.auger@ens.psl.eu

ATTESTATION

Je soussigné, Alain COCO, Responsable du pôle enseignants et chercheurs au Service des Ressources Humaines de l'École Normale Supérieure, atteste que

Monsieur David NACCACHE

né le 21 février 1967 à Beer-Sheva (ISRAEL)

est recruté, depuis le 30 septembre 2015, en qualité de Professeur des Universités, au sein de notre établissement.

Cette attestation est délivrée pour servir et valoir ce que de droit.

Fait à Paris, le 23/01/2025

Pour le Directeur de l'école normale supérieure
et par délégation
Le responsable RH du pôle des enseignants
et des chercheurs

Alain COCO