Articles scientifiques (liste partielle)

1. 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)

2. Houda Ferradi and Rémi Géraud and David Naccache and Assia Tria : When Organized Crime Applies Academic Results - A Forensic Analysis of an In-Card Listening Device. IACR Cryptology ePrint Archive 2015: 963 (2015)

3. Ehsan Aerabi and A. Elhadi Amirouche and Houda Ferradi and Rémi Géraud David Naccache and Jean Vuillemin: The Conjoined Microprocessor. IACR Cryptology ePrint Archive 2015: 974 (2015)

4. Diana Maimut, David Naccache, Rodrigo Portella do Canto, and Emil Simion Applying Cryptographic Acceleration Techniques to Error Correction, Proceedings of SECITC 2015, to appear in Springer LNCS 2015.

5. Eric Brier, Jean-Sébastien Coron, Rémi Géraud, Diana Maimut and David Naccache, A Number-Theoretic Error-Correcting Code, Proceedings of SECITC 2015, to appear in Springer LNCS 2015.

6. Céline Chevalier, Damien Gaumont, David Naccache, How to (Carefully) Breach a Service Contract?, Festschrift for David Kahn volume. Springer LNCS 9100 (to appear).

7. 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 (to appear).

8. Pierre-Alain Fouque, Sylvain Guilley, Cédric Murdica and 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 (to appear).

9. Houda Ferradi, Rémi Géraud, Diana Maimut, David Naccache and Hang Zho, Backtracking-Assisted Multiplication IACR Cryptology ePrint Archive 2015: 787 (2015). Festschrift for David Kahn volume. Springer LNCS 9100 (to appear).

10. Jean-Michel Cioranesco, Roman Korkikian, David Naccache and Rodrigo Portella do Canto, Buying AES Design Resistance with Speed and Energy, IACR Cryptology ePrint Archive 2015: 768 (2015). Festschrift for David Kahn volume. Springer LNCS 9100 (to appear).

11. Rémi Géraud, Diana Maimut and David Naccache, Double-Speed Barrett Moduli, IACR Cryptology ePrint Archive 2015: 785 (2015). Festschrift for David Kahn volume. Springer LNCS 9100 (to appear).

12. 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 DOI 10.1007/s10207-014-0272-7, January 2015.

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

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

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

16. 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

17. 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

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

19. 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)

20. 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)

21. 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)

22. 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

23. 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)

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

25. 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

26. 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)

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

28. 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)

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

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

31. 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)

32. 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

33. 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

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

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

36. 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

37. 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

38. 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)

39. 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)

40. 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)

41. 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)

42. 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)

43. 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)

44. 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)

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

46. 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)

47. 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)

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

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

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

51. 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)

52. 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

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

54. 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)

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

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

57. 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)

58. 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)

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

60. Julien Cathalo, David Naccache, Jean-Jacques Quisquater: Comparing with RSA. IMA Int. Conf. 2009: 326-335

61. Antoine Joux, Reynald Lercier, David Naccache, Emmanuel Thomé: Oracle-Assisted Static Diffie-Hellman Is Easier Than Discrete Logarithms. IMA Int. Conf. 2009: 351-367

62. 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)

63. Julien Cathalo, David Naccache, Jean-Jacques Quisquater: Comparing With RSA. IACR Cryptology ePrint Archive 2009: 21 (2009)

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

65. 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)

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

67. Antoine Joux, Reynald Lercier, David Naccache, Emmanuel Thomé: Oracle-Assisted Static Diffie-Hellman Is Easier Than Discrete Logarithms. IACR Cryptology ePrint Archive 2008: 217 (2008)

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

69. 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)

70. 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)

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

72. 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)

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

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

75. 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)

76. 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)

77. 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)

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

79. 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)

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

81. 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)

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

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

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

85. 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 juin 2004. Pages 330-342. Cryptology ePrint Archive, Report 2004/100. Also How to explain fault attacks to your kids, par 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)

86. 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.

87. 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

88. 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)

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

90. 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.

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

92. 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)

93. 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.

94. 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

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

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

97. 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.

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

99. 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

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

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

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

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

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

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

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

107. 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)

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

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

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

111. 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)

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

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

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

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

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

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

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

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

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

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

122. Cryptographic smart-cards, par David Naccache et David M'Raïhi IEEE Micro, 16(3):14-24, 1996. David Naccache, David M'Raïhi: 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.

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

124. David Naccache, A note about Σk^m k!, The Pentagon, vol. 49, no.2, pp. 10-15, 1990.

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

126. David Naccache, Michael Tunstall and 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

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

128. 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)

129. 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, par, In CardTech/SecurTech, pp. 99-104, Rockville, MD, USA, 1994, CTST Inc.

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

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

132. 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

133. 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

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

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

136. Proposal for a recurrent enumeration of all the permutations on any set of mutually disjoint elements, par David Naccache, 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.

Livres

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

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

Norme Internet (IETF)

139. 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.

Thèses & rubriques d'encyclopédie

140. David Naccache: Encyclopedia of Cryptography and Security (2nd Ed.) 2011 rubriques:

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

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

142. 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

Edition d'actes & d'ouvrages collectifs

143. 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

144. 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

145. 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

146. 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

147. 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

148. 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

149. 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

150. 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

151. 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

152. 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

153. 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

154. 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

Brevets d'invention (liste partielle)

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

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

3. David Naccache, Patrice Fremanteau, Unforgeable identification device, identification device reader and method of identification. US5434917 EP0583709

4. 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

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

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

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

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

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

10. 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

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

12. 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

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

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

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

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

17. 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

18. 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

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

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

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

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

23. 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

24. 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

25. 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

26. 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

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

28. 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

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

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

31. 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

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

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

34. 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

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

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

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

38. 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

39. 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

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

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

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

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

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

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

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

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

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

49. 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

50. 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

51. 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

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

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

54. 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

55. 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

56. David Naccache, Pascal Paillier, Support de mémorisation facilitant la saisie de caractères sur un combine de télephonie portable. Note: This invention, filed under the national reference number FR0401943 (item 21). It seems to have been withdrawn and does not appear on the espacenet database.

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

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

59. 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

60. 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

61. Brouchier Julien, Brier Eric; Naccache David, Dispositif de strockage de données sécurisé, WO2006128770 FR2886748

62. 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

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

64. 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

65. Naccache David, Procédé de protection contre le vol de terminaux, système, terminal et produit programme d'ordinateur correspondants. FR2924846 EP2068289 US2009151010 US8182549

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

67. Naccache David, Terminal de paiement électronique et procédé de mise à disposition de terminaux de paiement, FR2905022 US2008046381 EP1912168

68. 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.

69. Naccache David, Procédé de détection de cartes à microprocesseur non authentiques, cartes à microprocesseur, terminal lecteur de carte et programmes correspondants. FR2927454 EP2091028 US2009200372 US7971785.

70. Naccache David, Dolique Christophe, Procédé de contrôle d'accès, dispositif et produit programme d'ordinateur correspondants. FR2927452 EP2091025 US2009224872

71. Naccache David, Procédé de traçabilité d'un terminal de paiement électronique, en cas de vol de ce dernier, programme d'ordinateur et terminal correspondants. FR2927446 EP2091017 US2009207021 US8106771

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

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

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

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

76. Naccache David, Procédé de fabrication d'un terminal de paiement portable, terminal, dispositif et batterie correspondants. FR2922399 EP2048733 US2009095808

77. Naccache David, Procédé d'authentification, objet portatif et programme d'ordinateur correspondants. FR2922394 EP2048631 US2009100240 CA2640916 BRPI0804240

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

79. 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

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

81. Naccache David, Troumelin Michaël, Terminal de paiement, procédé et programme associés. FR2915302 EP1983480 US2008257954 US8074872.

82. Naccache David, Procédé de sécurisation et dispositif mobile ainsi sécurisé. FR2913296

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

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

85. Naccache David, Procédé de vérification de conformité d'une plateforme électronique et/ou d'un programme informatique présent sur cette plateforme, dispositif et programme d'ordinateur correspondants. FR2910657 EP1942428 US2008155507 US8171456

86. Naccache David, Procédé de vérification de la conformité du contenu logique d'un appareil informatique à un contenu de référence. EP1830295, WO2007099224. US2009260084 EP1830293 DE202006020631

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

88. Naccache David, Procédé de fourniture de données de transactions, terminal, procédé de transaction, procédé d'enrichissement de relevés bancaires, serveur, signaux et produits programme d'ordinateur correspondants. US2008103912 FR2907942 EP1916623 US8219469

89. Naccache David, Terminal avec afficheur et clavier de touches mécaniques. FR2907927.

90. Naccache David, Procédé d'impression de tickets. FR2907577, FR2907576, EP2084678. US2010044425 US8556171 WO2008049998 EP2A084678 ES2547227

91. Naccache David, Ecran tactile et terminal de paiement comprenant cet écran. FR2907563.

92. Naccache David, Dispositif d'alarme comprenant un terminal de paiement électronique et utilisation de ce dispositif. FR2905503 EP1903527 US2008055107

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

94. Naccache David, Biometric electronic payment terminal and transaction method. WO2008023114 US2010030696 FR2905187 EP2082364

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

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

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

98. 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.

99. 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.

100. Naccache David, Ticket printing method for electronic payment terminal e.g. computer, involves printing ticket relative to realized transaction after each transaction of payment, where ticket comprises already imprinted information. FR2907577.

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

103. Naccache David, Procédé et dispositif d'authentification d'un utilisateur. FR2902253 EP1868316 US2008077977 JP2007336546 CN101090322

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

105. 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

106. 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

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

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

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

110. Cioranesco Jean-Michel, Naccache David, Protection d'un circuit intégré contre des attaques invasives. FR2956760

111. 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

112. 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

113. 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.

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

115. Naccache David, Method of fighting ticket theft, corresponding ticket, deactivation device and activation device. AT518218 EP1916631 US2008100449 US7800502 FR2907948

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

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

118. 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

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

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

121. Naccache David, Terminal, method of checking conformity of at least one removable battery of an electronic payment terminal, and the corresponding removable battery and computer program product. US2009230180 US8074888 EP2099089 FR2928515

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

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

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

125. Naccache David, Method of securing a computer program and corresponding device, method of updating and update server. US2009204952 EP2090984 FR2927436 ES2349908 AT475933

126. Naccache David, Dabbous Nora, Method for securing a microprocessor, corresponding computer program and device. US2009172268 EP2079034 PT2079034 FR2925968 ES2391676

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

128. Naccache David, Biometric authentication method, computer program, authentication server, corresponding terminal and portable object. US2009100269 EP2048814 FR2922396 CA2640915 BRPI0804264

129. Naccache David, Biometric authentication method, authentication system, corresponding program and terminal. US2009097714. US8577090 EP2048592 FR2922340 ES2349359 CA2640856 BRPI0804241 AT475143

130. Naccache David, Method of transmitting a secret code, card reading terminal, management server and corresponding computer software programmes. US2009095809 EP2048632 FR2922395 CA2640945

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

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

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

134. Naccache David, Securing method and mobile device thus secured. US2008218347 EP1965328 FR2913296 HRP20150236

135. Naccache David, Integrated circuit and the corresponding test method, computer device and program. US2008195345 US7966145 EP1959266 FR2912551

136. Naccache David, Hardware security module, commissioning method and electronic payment terminal using this module. US2008163376. EP1944723 FR2910991 ES2330156

137. 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

138. Naccache David, Object's electronic bid managing server for online commerce field, has extension time period generating unit generating bid extension period that is not known to users, and control unit controlling display of information on user terminals. FR2925733.

139. 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

140. Naccache David, Method of printing receipts. US2010044425. US8556171 FR2907576 WO2008049998 EP2084678

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

142. Achari Karim, Naccache David, Procédé de contrôle d'une identité d'un terminal de paiement et terminal ainsi sécurisé, numéro de demande 1362564, numéro de soumission 1000219722. FR3015077

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

144. David Naccache, Magnetic head for a payment terminal, WO2015110610 FR3016994

145. David Naccache, Method of transmitting encrypted data, method of reception, devices and computer programs corresponding thereto, WO2015107175 FR3016762

146. David Naccache, Nora Dabbous, Device for processing data from a contactless smart card, method and corresponding computer program. WO2015158621 FR3020167

147. 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

148. 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

149. 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

150. 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