Curriculum Vitæ

Prof. Paulo L. Barreto, Ph.D., Hab.

Autumn 2022

Introduction

I was born in the city of Salvador, capital of the State of Bahia, Brazil (whence my Latino background), and I am an American citizen since September 2022. I obtained my BSc in Physics in 1987, received my Ph.D. degree in Engineering in 2003 (thesis title: "*Robust Cryptography and Fragile Watermarks: Construction and Analysis of Algorithms to Locate Changes in Digital Images*") and my Habilitation (higher doctorate) in Computer Engineering in 2011 (thesis title: "*Construction of Parameters and Efficient Algorithms for Post-Quantum Cryptosystems Based on Coding Theory*"), all at the University of São Paulo.

I worked at Unisys Brazil Ltd (1990–1997) as systems software analyst and developer, then as independent security consultant and systems software developer (1998–1999), and finally at and Scopus Tecnologia S/A (1999–2004) as chief cryptographer. Overall, I have had 15 (fifteen) years of experience in industry before I began the academic part of my career, and I have kept close contact with industry ever since, as one of my professional tenets as a cryptographer is that good cryptography stems from directly observed, perceived, or actively foreseen needs from the industrial, governmental, and societal realms.

I collaborated with the MBA in Information Technologies and Communication at the Escola Politécnica of the University of São Paulo from 2002 to 2004. I joined the faculty at the Department of Computer and Digital Systems Engineering, Escola Politécnica, University of São Paulo in December 2004 as Assistant Professor, and became Associate Professor there in October 2011. I joined the faculty at the School of Engineering and Technology, University of Washington Tacoma as Assistant Professor in September 2015 and was tenured and promoted to Associate Professor in 2022 (formal letter from the President and the Provost received March 2022, effective September 2022). My academic experience is thus 20 years long and counting.

I am one of the designers of the WHIRLPOOL hash function standardized in ISO/IEC 10118-3, as well as several other symmetric primitives (block ciphers, authenticated encryption modes and key derivation functions). I have co-authored extensive research work on elliptic curve cryptography and pairing-based cryptography, including efficient bilinear pairing algorithms (e.g. the BKLS and η_T techniques), identity-based cryptographic protocols (e.g. the BLMQ signature and signcryption methods), and the construction of pairing-friendly elliptic curves (e.g. the BN and BLS families of elliptic curves), many of them standardized in ISO-IEC 15946-5 and adopted in influential applications like cryptocurrencies. More recently I have been working on efficient algorithms and protocols for quantum-resistant (also called post-quantum) cryptosystems, including code-based, lattice-based, hash-based, and supersingular isogeny-based schemes. I am co-author of a 3rd-round alternate algorithm submitted to the ongoing

NIST Post-Quantum standardization process (the code-based BIKE protocol), and my research has positively impacted another submission (the isogeny-based SIKE key agreement scheme). I also co-authored two other NIST post-quantum proposals, the qTESLA lattice-based digital signature scheme and the DAGS code-based key agreement scheme.

I have served in 30 PhD defense committees and 31 MSc defense committees since 2005. I supervised to completion 4 PhD theses (since 2010), 10 MSc theses (since 2008) and one Honors thesis (since 2020), with one further PhD student currently under my supervision. I also served in the program committees of over 90 conferences, and I am a member of the Steering Committee of the Latincrypt series of conferences (whose first installment I co-chaired) and the ASCrypto series of advanced schools in cryptography. I completed a 3-year term as Associate Editor of IET Information Security (2015–2018), two 4-year terms as Associate Editor of the Journal of Cryptographic Engineering (2011–2014, 2015–2018), a 4-year term as Associate Editor of IEEE Transactions on Computers (2015–2019, including an extension of a few months beyond the usual maximum duration at a personal request from the Editor-in-Chief; Publons lists 31 verified editor records for this assignment as Associate Editor; and starting in 2022 I am currently serving a 5-year term as Associate Editor of the IACR Journal of Cryptology.

Honors

The paper “Efficient Algorithms for Pairing-Based Cryptosystems” (Advances in Cryptology – Crypto 2002, LNCS **2442**, 354–368, Springer, 2002), which I jointly wrote with three co-authors, was identified in March 2005 as a Hot Paper by Thomson ISI®'s Essential Science Indicators, by virtue of being among the top one-tenth of one percent (0.1%) most cited papers in the Computer Science category. The same paper was recognized by Thomson ISI®'s Essential Science Indicators in December 2005 as a Fast Breaking Paper, for having the largest percentage increase in citations among the 1% most cited papers in its category.

My students and I were granted the following awards:

- Best Paper Award at the 22th Brazilian Symposium on Information and Computer Systems Security (SBSeg 2022).
- Best MSc Thesis Supervision Award at the 16th Brazilian Symposium on Information and Computer Systems Security (SBSeg 2016).
- Runner-up MSc Thesis Supervision Award at the 14th Brazilian Symposium on Information and Computer Systems Security (SBSeg 2014).
- Runner-up Reviewer Award at the 14th Brazilian Symposium on Information and Computer Systems Security (SBSeg 2014).
- Runner-up for Best PhD Thesis Supervision in Engineering at the Brazilian national level, CAPES Foundation, 2011.
- Best PhD Thesis Supervision Award at the 10th Brazilian Symposium on Information and Computer Systems Security (SBSeg 2010).
- Best MSc Thesis Supervision Award at the 10th Brazilian Symposium on Information and Computer Systems Security (SBSeg 2010).

- Best Paper Award at the 8th Brazilian Symposium on Information and Computer Systems Security (SBSeg 2008).
- Best Paper Award at the 16th International Symposium on Undergraduate Research of the University of São Paulo (SIICUSP 2008).
- Best Paper Award at the 25th Brazilian Symposium on Computer Networks and Distributed Systems (SBRC 2007).
- Best Paper Award at the 6th Brazilian Symposium on Information and Computer Systems Security (SBSeg 2006).

I was also granted the Research Productivity Award level 2 in 2006 for the following 3 years by the Brazilian National Council for Scientific and Technological Development (CNPq). That award was granted again in 2009 for the following 3 years and promoted to level 1D in 2012 for the following 4 years. In May 2008 I was granted the E. T. S. Walton Award by the Science Foundation Ireland (SFI), process 07/W.1/I1824.

I have given over 30 invited/keynote talks, including Distinguished Keynote Speaker at the 20th anniversary Selected Areas in Cryptography conference (2013) and the most recent having taken place during the 20th anniversary Brazilian Symposium on Information and Computational Systems Security (SBSeg 2020) in October 2020. I have been honored with the Latinx Faculty Recognition Award 2017 and 2019 from the University of Washington (tri-campus).

My Hirsch Index (*h*-index) is 40 according to Google Scholar (10190 citations for about 150 works, profile ID: kG_95CgAAAAJ); 34 according to Semantic Scholar (7217 citations for 116 works, https://www.semanticscholar.org/author/Paulo-S.-L.-M.-Barreto/1698800); 23 according to Scopus (4110 citations for 72 works, Scopus author ID: 7004230957); and 21 according to the Web of Science (2962 citations for 60 works, ResearcherID: F-5788-2010).

Teaching activities

My teaching experience extends from the early 2000's to the present, although occasional teaching activities could be traced back to the early 1990's. Over 12 years, I taught the following courses at the University of São Paulo:

- Elliptic Curve & Pairing-Based Cryptography (grad level)
- Post-Quantum Cryptography (grad level)
- Quantum Cryptography (grad level)
- Network & Information Security (grad level)
- Information Security (undergrad level)
- Computer Systems Performance Evaluation (undergrad level)
- Computer Networks (undergrad level)

I have taught (or am currently teaching) the following courses at UW Tacoma:

- TCSS 342 Data Structures (Spring 2018, Spring 2019 [2 sections], Spring 2020, Spring 2022; undergrad level).

- TCSS 343 Design and Analysis of Algorithms (Autumn 2015, Winter 2016, Spring 2016, Autumn 2016, Winter 2017, Spring 2017, Autumn 2017, Autumn 2019, Winter 2020, Autumn 2020, Winter 2021 [2 sections], Autumn 2021, Winter 2022, Autumn 2022; undergrad level).
- TCSS 543 Advanced Algorithms (Winter 2016, Summer 2016, Winter 2017, Winter 2018, Summer 2018, Autumn 2018, Autumn 2019, Autumn 2020, Summer 2021, Autumn 2021, Autumn 2022; grad level).
- TCSS 421 Compiler Construction (Spring 2016, Spring 2017, Winter 2018, Autumn 2018; undergrad level).
- TCSS 487 Cryptography (Spring 2018, Spring 2019, Winter 2020, Summer 2020, Spring 2021, Spring 2022; undergrad level).

TCS 421 Compiler Construction is a course I revised and renewed entirely, adopting the far more modern approach to the subject proposed by Campbell, Iyer, and Akbal-Delibaş in their 2012 (1st edition) textbook "*Introduction to Compiler Construction in a Java World*," that mimics the typical compiler development scenarios actually found in industry, namely, a large and theoretically sophisticated, but also incremental and tool-based, software engineering project.

Furthermore, I collaborated with the following course:

- TCSS 595: Research Seminar in Cybersecurity (Winter 2016; grad level).

I have also been responsible for the following formal courses:

- TCSS 390 Undergraduate Seminar in CSS (Summer 2016).
- TCSS 497 Internship in Computing and Software Systems (Spring 2016, Summer 2016, Winter 2017, Spring 2017).
- TCSS 499 Undergraduate Research in Computing and Software Systems (Spring 2018, Summer 2020, Autumn 2020).
- TCSS 600 Independent Study or Research (Summer 2018, Autumn 2020).
- TCSS 700 Masters' Thesis (Spring 2018, Spring 2019, Summer 2019, Autumn 2019, Winter 2020, Winter 2022, Spring 2022, Summer 2022).

I also designed a new grad-level course, TCSS 583 Post-Quantum Cryptography. This is an entirely updated version of a similar course I had designed and taught at the University of São Paulo (2008 to 2015).

I have been a member of the CSS Undergraduate Committee and the MCSS Graduate Committee at the School of Engineering and Technology of the University of Washington Tacoma since I joined the faculty. I also collaborate with the researchers of the Center for Data Science of the University of Washington Tacoma along the research area of Secure Machine Learning.

Research interests

My research interests in cryptography are completely eclectic. All individual research targets (from the most theoretical to the essentially practical) are anchored in real-world needs.

This includes (but is not restricted to) the following topics, all of which are represented one or more times among my published and submitted papers:

- Design and analysis of block ciphers, modes of operation for block ciphers, and hash functions;
- Cryptographic sponges and password derivation schemes;
- Construction of pairing-friendly elliptic curves;
- Efficient and side-channel-resistant algorithms for cryptosystems based on elliptic curves and bilinear pairings;
- Identity-based key agreement protocols, digital signatures and signcryption from elliptic curves and bilinear pairings;
- Code-based encryption and key agreement schemes, and design of secure supporting error-correcting codes;
- Hash-based digital signatures;
- Lattice-based cryptosystems and digital signatures;
- Supersingular isogeny-based cryptosystems and efficient supporting algorithms.

Peer-reviewed journal papers

1. BARRETO, P. S. L. M.; Simplicio Jr, M. A.; Ricardini, J. E.; Patil, H. K.: "Schnorr-based implicit certification: improving the security and efficiency of vehicular communications." *IEEE Transactions on Computers* 70(3), pp. 393–399, IEEE, March 2021 (early online access: 2020), DOI: 10.1109/TC.2020.2988637 – *equal contribution on all aspects*.
2. Banegas, G.; BARRETO, P. S. L. M.; Persichetti, E.; Santini, P.: "Designing Efficient Dyadic Operations for Cryptographic Applications." *Journal of Mathematical Cryptology* v. 14, n. 1, pp. 95–109, DeGruyter, June 2020, DOI: 10.1515/jmc-2015-0054 (extended version of conference paper published at MathCrypt 2018 conference) – *equal contribution on all aspects*.
3. Zanon, G. H. M.; Simplicio Jr, M. A.; Pereira, G. C. C. F.; Doliskani, J.; BARRETO, P. S. L. M.: "Faster Key Compression for Isogeny-Based Cryptosystems." *IEEE Transactions on Computers*, v. 68, n. 5, p. 688–701, DOI: 10.1109/TC.2018.2878829, 2018 (electronic version), 2019 (printed version). – *equal contribution on all aspects.*
4. Banegas, G.; BARRETO, P. S. L. M.; Boidje, B. O.; Cayrel, P.-L.; Dione, G. N.; Gaj, K.; Gueye, C. T.; Haeussler, R.; Klamti, J. B.; Ndiaye, O.; Nguyen, D. T.; Persichetti, E.; Ricardini, J. E.: "DAGS: Key encapsulation using dyadic GS codes." *Journal of Mathematical Cryptology*, v. 12, n. 4, p. 221–239, DeGruyter, DOI: 10.1515/jmc-2018-0027, 2018. – *equal contribution on all aspects.*
5. Farias, L. A.; Albertini, B. C.; BARRETO, Paulo S. L. M.: "A class of safe and efficient binary Edwards curves." *Journal of Cryptographic Engineering*, v. 8, p. 1–13, DOI: 10.1007/s13389-017-0174-5, 2018. – *supervised research.*
6. Andrade, E.; Simplicio Jr., M.; BARRETO, P. S. L. M.; Santos, P.: "Lyra2: efficient password hashing with high security against time-memory trade-offs." *IEEE Transactions on Computers*, v. 65, p. 3096–3108. DOI: 10.1109/TC.2016.2516011, 2016 – *equal contribution on all aspects.*

7. Pereira, G. C. C. F.; Puodzius, C. O.; BARRETO, P. S. L. M.: “Shorter Hash-Based Signatures.” *The Journal of Systems and Software*, v. 116, p. 95–100, DOI: 10.1016/j.jss.2015.07.007, 2015 – *supervised research*.
8. Massolino, P. M. C.; BARRETO, P. S. L. M.; Ruggiero, W. V.: “Optimized and Scalable Co-Processor for McEliece with Binary Goppa Codes.” *ACM Transactions on Embedded Computing Systems*, v. 14, p. 1–32, DOI: 10.1145/2736284, 2015. – *equal contribution on all aspects.*
9. Possignolo, R. T.; Margi, C. B.; BARRETO, P. S. L. M.: “Quantum-assisted QD-CFS signatures.” *Journal of Computer and System Sciences*, v. 81, p. 458–467, DOI: 10.1016/j.jcss.2014.10.003, 2015. – *equal contribution on all aspects.*
10. Barguil, J. M. M.; BARRETO, P. S. L. M.: “Security issues in Sarkar’s e-cash protocol.” *Information Processing Letters*, v. 115, n. 11, p. 801–803, DOI: 10.1016/j.ipl.2015.06.007, 2015. – *supervised research.*
11. Almeida, L. C.; Andrade, E. R.; BARRETO, P. S. L. M.; Simplicio Jr., M. A.: “Lyra: password-based key derivation with tunable memory and processing costs.” *Journal of Cryptographic Engineering*, v. 4, n. 2, p. 75–89, DOI: 10.1007/s13389-013-0063-5, 2014. – *equal contribution on all aspects.*
12. Biasi, F. P.; BARRETO, P. S. L. M.; Misoczki, R.; Ruggiero, W. V.: “Scaling efficient code-based cryptosystems for embedded platforms.” *Journal of Cryptographic Engineering*, v. 4, n. 2, p. 123–134, DOI: 10.1007/s13389-014-0070-1, 2014. – *supervised research.*
13. Pereira, G. C. C. F.; Santos, M. A. S.; de Oliveira, B. T.; Simplicio Jr., M. A.; BARRETO, P. S. L. M.; Margi, C. B.; Ruggiero, W. V.: “SMSCrypto: A Lightweight Cryptographic Framework for Secure SMS Transmission.” *The Journal of Systems and Software*, v. 86, p. 698–706, DOI: 10.1016/j.jss.2012.11.004, 2013. – *equal contribution on all aspects.*
14. Simplicio Jr., M. A.; de Oliveira, B. T.; Margi, C. B.; BARRETO, P. S. L. M.; Carvalho, T. C. M. B.; Näslund, M.: “Survey and comparison of message authentication solutions on wireless sensor networks.” *Ad Hoc Networks*, v. 11, p. 1221–1236, DOI: 10.1016/j.adhoc.2012.08.011, 2013. – *analysis of cryptographic protocols.*
15. BARRETO, P. S. L. M.; Misoczki, R.; Lindner, R.: “Decoding Square-Free Goppa Codes Over $\mathbb{F}_p$.” *IEEE Transactions on Information Theory*, v. 59, p. 6851–6858, DOI: 10.1109/TIT.2013.2270272, 2013. – *equal contribution on all aspects.*
16. Simplicio Jr., M. A.; BARRETO, P. S. L. M.: “Revisiting the Security of the ALRED Design and Two of Its Variants: Marvin and LetterSoup.” *IEEE Transactions on Information Theory*, v. 58, p. 6223–6238, DOI: 10.1109/TIT.2012.2203093, 2012. – *supervised research.*
17. BARRETO, P. S. L. M.; Misoczki, R.; Simplicio Jr., Marcos A.: “One-time signature scheme from syndrome decoding over generic error-correcting codes.” *The Journal of Systems and Software*, v. 84, p. 198–204, DOI: 10.1016/j.jss.2010.09.016, 2011. – *equal contribution on all aspects.*
18. Pereira, G. C. C. F.; Simplicio Jr., M. A.; Naehrig, M.; BARRETO, P. S. L. M.: “A Family of Implementation-Friendly BN Elliptic Curves.” *The Journal of Systems and Software*, v. 84, p. 1319–1326, DOI: 10.1016/j.jss.2011.03.083, 2011. – *supervised research.*
19. BARRETO, P. S. L. M; Nikov, V.; Nikova, S.; Rijmen, V.; Tischhauser, E.: “Whirlwind: a new cryptographic hash function.” *Designs, Codes and*

Cryptography, v. 56, p. 141–162, DOI: 10.1007/s10623-010-9391-y, 2010. – *equal contribution on all aspects.*

20. Simplicio Jr., M. A.; BARRETO, P. S. L. M.; Margi, C. B.; Carvalho, T. C.M.B.: “A survey on key management mechanisms for distributed Wireless Sensor Networks.” *Computer Networks*, v. 54, p. 2591–2612, DOI: 10.1016/j.comnet.2010.04.010, 2010. – *analysis of cryptographic protocols.*
21. Maia, R. J. M.; BARRETO, P. S. L. M.; de Oliveira, B. T.: “Implementation of Multivariate Quadratic Quasigroup for Wireless Sensor Network.” *Transactions on Computational Science* (Print), v. XI, p. 64–78, DOI: 10.1007/978-3-642-17697-5_4, 2010. – *supervised research.*
22. Simplicio Jr., MA.; Barbuda, P. A. F. F. S.; BARRETO, P. S. L. M.; Carvalho, T. C. M. B.; Margi, C. B.: “The Marvin Message Authentication Code and the LetterSoup Authenticated Encryption Scheme,” *Security and Communication Networks* v. 2, n, 2. p. 165–180, Wiley Interscience, DOI: 10.1002/sec.66, 2009. – *supervised research.*
23. Kobayashi, L. O. M.; Furuie, S. S.; BARRETO, P. S. L. M.: “Providing Integrity and Authenticity in DICOM Images: a Novel Approach.” *IEEE Transactions on Information Technology in Biomedicine*, v. 13, p. 582–589, DOI: 10.1109/TITB.2009.2014751, 2009. – *analysis of cryptographic protocols.*
24. Misoczki, R.; BARRETO, P. S. L. M.: “Criptografia Pós-Quântica com Códigos Corretores de Erros.” *REIC. Revista Eletrônica de Iniciação Científica* (in Portuguese), v. 9, p. 1–20, 2009. – *supervised research.*
25. Rijmen, V.; BARRETO, P. S. L. M.; Gazzoni Filho, D. L.: “Rotation symmetry in algebraically generated cryptographic substitution tables.”, *Information Processing Letters* v. 106, p. 246–250, DOI: 10.1016/j.ipl.2007.09.012, 2008. – *supervised research.*
26. BARRETO, P. S. L. M.; Galbraith, S.; Ó hÉigeartaigh, C.; Scott, M.: “Efficient Pairing Computation on Supersingular Abelian Varieties.” *Designs, Codes and Cryptography* v. 42, p. 239–271, DOI: 10.1007/s10623-006-9033-6, 2007. – *equal contribution on all aspects.*
27. Ronan, R.; Murphy, C.; Kerins, T.; Ó hÉigeartaigh, C., BARRETO, P. S. L. M.: “A flexible processor for the characteristic 3 η_T pairing.” *International Journal of High Performance Systems Architecture* v. 1, p. 79–88, DOI: 10.1504/IJHPSA.2007.015393, 2007. – *equal contribution on all aspects.*
28. Vieira, G. Y. M.; BARRETO, P. S. L. M.; Ruggiero, W. V.: “The SACI Special-Purpose Block Cipher.” *Revista de Engenharia de Computação e Sistemas Digitais*, v. 3, p. 63–74, n3/r003a006, 2007. – *equal contribution on all aspects.*
29. Scott, M., BARRETO, P. S. L. M.: “Generating more MNT elliptic curves.” *Designs, Codes and Cryptography* v. 38, p. 209–217, DOI: 10.1007/s10623-005-0538-1, 2006. – *equal contribution on all aspects.*
30. BARRETO, P. S. L. M.; Voloch, F.: “Efficient Computation of Roots in Finite Fields.” *Designs, Codes and Cryptography* v. 39, p. 275–280, DOI: 10.1007/s10623-005-4017-5, 2006. – *equal contribution on all aspects.*
31. Kerins, T.; Marnane, W.; Popovici, E.; BARRETO, P. S. L. M.: “Hardware Accelerators for Pairing Based Cryptosystems. *IEE Proceedings on Information Security* v. 152, p. 47–56, DOI: 10.1049/ip-ifs:20055009, 2005. – *equal contribution on all aspects.*
32. BARRETO, P. S. L. M.; Kim, H. Y.: “Fast hashing onto pairing-friendly elliptic curves over ternary fields.” *Revista de Engenharia de Computação e Sistemas Digitais* v. 2, p. 19–28, n2/r002a002, 2005. – *equal contribution on all aspects.*

33. BARRETO, P. S. L. M.; Lynn, B.; Scott, M.: “Efficient Implementation of Pairing-Based Cryptosystems.” *Journal of Cryptology* v. 17, p. 321–334, DOI: 10.1007/s00145-004-0311-z, 2004. – *equal contribution on all aspects.*
34. BARRETO, P. S. L. M.: “Aspecto e comprometimento: nota sobre antropologia e gramática” (in Portuguese), *Videtur* v. 28, p. 33–34, videtur28_04, 2004. – *individual research.*
35. BARRETO, P. S. L. M.; Kim, H. Y.; Rijmen, V.: “Toward a Secure Public-Key Blockwise Fragile Authentication Watermarking.” *IEE Proceedings on Vision, Image and Signal Processing* v. 149, p. 57–62, DOI: 10.1109/ICIP.2001.958536, 2002. – *equal contribution on all aspects.*

Peer-reviewed conference papers

1. Doliskani, J., Pereira, G. C. C. F.; BARRETO, P. L.: “Faster Cryptographic Hash Function From Supersingular Isogeny Graphs,” Selected Areas in Cryptography – SAC 2022, Lecture Notes in Computer Science: Springer, to appear, August 2022. – *equal contribution on all aspects*.
2. BARRETO, P. L.; Zanon, G. H. M.; Simplicio Jr, M. A.: “Succinct Non-interactive Arguments of Knowledge from Supersingular Isogenies,” Proceedings of the XXII Brazilian Symposium on Information and Computational Systems Security – SBSeg 2022, 2022. – *equal contribution on all aspects*.
3. Pereira, G. C. C. F.; BARRETO, P. S. L. M.: “Isogeny-Based Key Compression Without Pairings,” International Conference on Practice and Theory of Public-Key Cryptography (PKC 2021) Part 1, Lecture Notes in Computer Science 12170, p. 131–154, Springer, DOI: 10.1007/978-3-030-75245-3_6, May 2021.
4. Aragon, N.; BARRETO, P. S. L. M.; Bettaieb, S.; Bidoux, L.; Blazy, O.; Deneuville, J.-C.; Gaborit, P.; Ghosh, S.; Gueron, S.; Güneysu, T.; Aguilar-Melchor, C.; Misoczki, R.; Persichetti, E.; Richter-Brockmann, J.; Sendrier, N.; Tillich, J.-P.; Vasseur, V.; Zémor, G.: “BIKE: Bit Flipping Key Encapsulation (3rd round update),” 3rd NIST Post-Quantum Cryptography Standardization Conference, June 2021. – *equal contribution on all aspects.*
5. Alkim, E.; BARRETO, P. S. L. M.; Bindel, N.; Krämer, J.; Longa, P.; Ricardini, J. E.: “The Lattice-Based Digital Signature Scheme qTESLA,” International Conference on Applied Cryptography and Network Security (ACNS 2020), Lecture Notes in Computer Science 12146, p. 441–460, Springer, DOI: 10.1007/978-3-030-57808-4_22, August 2020 – *equal contribution on all aspects*.
6. BARRETO, P. S. L. M.; Oliveira, G. A.; Benits, W.; Nascimento, A. C.: “Supersingular isogeny oblivious transfer,” Proceedings of the XIX Brazilian Symposium on Information and Computational Systems Security – SBSeg 2019. (available online at https://sbseg2019.ime.usp.br/anais/196020.pdf), 2019. – *supervised research*.
7. Akleylek, S.; Alkim, E.; BARRETO, P. S. L. M.; Bindel, N.; Buchmann, J.; Eaton, E.; Gutoski, G.; Kramer, J.; Longa, P.; Polat, H.; Ricardini, J. E.; Zanon, G.: “Lattice-based digital signature scheme qTESLA (updated),” 2nd NIST Post-Quantum Cryptography Standardization Conference, 2019. – *equal contribution on all aspects.*
8. Aragon, N.; BARRETO, P. S. L. M.; Bettaieb, S.; Bidoux, L.; Blazy, O.; Deneuville, J.-C.; Gaborit, P.; Gueron, S.; Güneysu, T.; Aguilar-Melchor, C.;

Misoczki, R.; Persichetti, E.; Sendrier, N.; Tillich, J.-P.; Zémor, G.: “BIKE: Bit Flipping Key Encapsulation (updated),” 2nd NIST Post-Quantum Cryptography Standardization Conference, 2019. – *equal contribution on all aspects.*

9. Banegas, G.; BARRETO, P. S. L. M.; Boidje, B. O.; Cayrel, P.-L.; Dione, G. N.; Gaj, K.; Gueye, C. T.; Haeussler, R.; Klamti, J. B.; Ndiaye, O.; Nguyen, D. T.; Persichetti, E.; Ricardini, J. E.: “DAGS Reloaded: Revisiting Dyadic Key Encapsulation,” Workshop on Code-Based Cryptography (CBC 2019), Lecture Notes in Computer Science, v. 11666, p. 69–85, Springer, DOI: 10.1007/978-3-030-25922-8_4, 2019. – *equal contribution on all aspects.*
10. Aragon, N.; BARRETO, P. S. L. M.; Bettaieb, S.; Bidoux, L.; Blazy, O.; Deneuville, J.-C.; Gaborit, P.; Gueron, S.; Güneysu, T.; Aguilar-Melchor, C.; Misoczki, R.; Persichetti, E.; Sendrier, N.; Tillich, J.-P.; Zémor, G.: “BIKE: Bit Flipping Key Encapsulation,” 1st NIST Post-Quantum Cryptography Standardization Conference, 2018. – *equal contribution on all aspects.*
11. Akleylek, S.; Alkim, E.; BARRETO, P. S. L. M.; Bindel, N.; Buchmann, J.; Eaton, E.; Gutoski, G.; Kramer, J.; Longa, P.; Polat, H.; Ricardini, J. E.; Zanon, G.: “Lattice-based digital signature scheme qTESLA,” 1st NIST Post-Quantum Cryptography Standardization Conference, 2018. – *equal contribution on all aspects.*
12. Banegas, G.; BARRETO, P. S. L. M.; Boidje, B. O.; Cayrel, P. L.; Dione, G. N.; Gaj, K.; Gueye, C. T.; Haeussler, R.; Klamti, J. B.; N’diaye, O.; Nguyen, D. T.; Persichetti, E.; Ricardini, J. E.: “DAGS: Key Encapsulation from Quasi-Dyadic Generalized Srivastava Codes,” 1st NIST Post-Quantum Cryptography Standardization Conference, 2018. – *equal contribution on all aspects.*
13. Banegas, G.; BARRETO, P. S. L. M.; Persichetti, E.; Santini, P.: “Designing Efficient Dyadic Operations for Cryptographic Applications,” Proceedings of the Mathematical Cryptography Workshop – MathCrypt 2018, Santa Barbara, CA, DOI: 10.1515/jmc-2015-0054, 2018. – *equal contribution on all aspects.*
14. Farias, L.; Albertini, B. C.; BARRETO, P. S. L. M.: “An approach to Elliptic Curve Cryptography with AOP oriented to Hardware,” Extended Proceedings of the 18th Brazilian Symposium on Information and Computational Systems Security (SBSeg CTD 2018), Porto Alegre, Brazil, p. 1–8. Brazilian Computer Society, 2018. – *supervised research.*
15. Zanon, G. H. M.; Simplicio Jr, M. A.; Pereira, G. C. C. F.; Doliskani, J.; BARRETO, P. S. L. M.: “Faster Isogeny-Based Compressed Key Agreement”, International Conference on Post-Quantum Cryptography – PQCrypto 2018, Fort Lauderdale (FL), USA. Lecture Notes in Computer Science, v. 10786, p. 248–268, Springer, DOI: 10.1007/978-3-319-79063-3_12, 2018. – *equal contribution on all aspects.*
16. BARRETO, P. S. L. M.; Gueron, S.; Güneysu, T.; Misoczki, R.; Persichetti, E.; Sendrier, N.; Tillich, J.-P.: “CAKE: Code-based algorithm for key encapsulation,” IMA International Conference on Cryptography and Coding – IMACC 2017, Oxford, UK. Lecture Notes in Computer Science, v. 10655, p. 207–226, Springer, DOI: 10.1007/978-3-319-71045-7_11, 2017. – *equal contribution on all aspects.*
17. Farias, L.; Albertini, B. C.; BARRETO, P. S. L. M: “Cryptographic architecture for co-process on consumer electronics devices.” In: IEEE International Symposium on Consumer Electronics, 2016, São Paulo, Brazil. Proceedings of the 20th IEEE International Symposium on Consumer Electronics, v. 1, p. 3–5, DOI: 10.1109/ISCE.2016.7797354, 2016. – *supervised research.*

18. Farias, L.; Albertini, B. C.; BARRETO, P. S. L. M.: “Parallelism Level Analysis of Binary Field Multiplication on FPGAs.” In: V Brazilian Symposium on Computing Systems Engineering (SBESC 2015), Foz do Iguaçu, Brazil. SBESC 2015 Proceedings, p. 64–69, DOI: 10.1109/SBESC.2015.19, 2015. – *supervised research.*
19. BARRETO, P. S. L. M.; Costello, C.; Misoczki, R.; Naehrig, M.; Pereira, G. C. C. F.; Zanon, G.: “Subgroup Security in Pairing-Based Cryptography.” In: 4th International Conference on Cryptology and Information Security in Latin America – Latincrypt 2015, Guadalajara, México. Lecture Notes in Computer Science, Berlin Heidelberg: Springer, v. 9230. p. 245–265, DOI: 10.1007/978-3-319-22174-8_14, 2015. – *equal contribution on all aspects.*
20. Barguil, J. M. M.; Lino, R. Y.; BARRETO, P. S. L. M.: “Efficient variants of the GGH-YK-M cryptosystem.” In: Brazilian Symposium on Information and Computer Systems Security – SBSeg 2014, Belo Horizonte, Brazil. Proceedings of the 14th Brazilian Symposium on Information and Computer Systems Security – SBSeg 2014. Brazilian Computer Society (SBC), 2014. – *supervised research.*
21. Massolino, P. M. C.; Margi, C. B.; BARRETO, P. S. L. M.; Ruggiero, W. V.: “Scalable Hardware Implementation for Quasi-Dyadic Goppa Encoder.” In: Proceedings of the 5th IEEE Latin American Symposium on Circuits and Systems – LASCAS 2014, Santiago, Chile, DOI: 10.1109/LASCAS.2014.6820285, 2014. – *equal contribution on all aspects.*
22. Misoczki, R.; Tillich, J.; Sendrier, N.; BARRETO, P. S. L. M.: “MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes.” In: Proceedings of the 2013 IEEE International Symposium on Information Theory - ISIT 2013, Istanbul, Turkey. Proceedings, p. 2069–2073, DOI: 10.1109/ISIT.2013.6620590, 2013. – *equal contribution on all aspects.*
23. Aranha, D. F.; Longa, P.; BARRETO, P. S. L. M.; Ricardini, J. E.: “The Realm of the Pairings.” In: Selected Areas in Cryptography – SAC 2013, Lecture Notes in Computer Science, Heidelberg: Springer. v. 8282. p. 3–25, DOI: 10.1007/978-3-662-43414-7_1, 2014. – *equal contribution on all aspects.*
24. Costa, C. H. A.; Moreira, J. E.; Januario, G. C.; BARRETO, P. S. L. M.: “Dynamic method to evaluate code optimization effectiveness.” In: Map2MPSoC/SCOPES 2012, 2012, Sankt Goar. Proceedings of the 15th International Workshop on Software and Compilers for Embedded Systems, p. 62–71, DOI: 10.1145/2236576.2236583, 2012. – *supervised research.*
25. Barbier, M.; BARRETO, P. S. L. M.: “Key Reduction of McEliece’s Cryptosystem Using List Decoding.” In: IEEE International Symposium on Information Theory – ISIT 2011, 2011, Sankt Petersburg, Russia. Proceedings of the 2011 IEEE International Symposium on Information Theory, p. 2681–2685, DOI: 10.1109/ISIT.2011.6034058, 2011. – *equal contribution on all aspects.*
26. Simplício Jr., M. A.; Oliveira, B. T.; Margi, C. B.; BARRETO, P. S. L. M.; Näslund, M.; Carvalho, T. C. M. B.: “Comparison of Authenticated-Encryption Schemes in Wireless Sensor Networks.” In: IEEE Conference on Local Computer Networks – LCN 2011, 2011, Bonn, Germany. Proceedings of the 36th IEEE Conference on Local Computer Networks – LCN 2011, p. 450–457, DOI: 10.1109/LCN.2011.6115506, 2011. – *analysis of cryptographic protocols*.
27. BARRETO, P. S. L. M.; Lindner, R.; Misoczki, R.: “Monoidic Codes in Cryptography.” In: International Conference on Post-Quantum Cryptography – PQCrypto 2011, 2011, Taipei, Taiwan. Proceedings of the 4th International Conference on Post-Quantum Cryptography – PQCrypto 2011. Lecture Notes in

Computer Science, v. 7071, p. 179–199, DOI: 10.1007/978-3-642-25405-5_12, 2011. – *equal contribution on all aspects.*

28. Margi, C. B.; Oliveira, B. T.; Sousa, G. T.; Simplicio Jr., M. A.; BARRETO, P. S. L. M.; Carvalho, T. C. M. B.; Näslund, M.; Gold, R.: "Impact of Operating Systems on Wireless Sensor Networks (Security) Applications and Testbeds." In: Proceedings of the International Conference on Computer Communication Networks (ICCCN 2010) / IEEE International Workshop on Wireless Mesh and Ad Hoc Networks (WiMAN 2010), Zürich, Switzerland, p. 1–6, DOI: 10.1109/ICCCN.2010.5560028, 2010. – *analysis of cryptographic protocols*.
29. BARRETO, P. S. L. M.; Cayrel, P.; Misoczki, R.; Niebuhr, R.: "Quasi-dyadic CFS signatures." In: International Conference on Information Security and Cryptology – Inscrypt 2010, Shanghai, China. Proceedings of the 6th International Conference on Information Security and Cryptology – Inscrypt 2010. Heidelberg: Springer, 2010. v. 6584, p. 336–349, DOI: 10.1007/978-3-642-21518-6_23, 2010. – *equal contribution on all aspects.*
30. Simplício Jr., M. A.; BARRETO, P. S. L. M.; Carvalho, T. C. M. B.: "Revisiting the Security of the ALRED Design." In: 13th Information Security Conference (ISC 2010), Boca Raton, FL. Lecture Notes in Computer Science, v, 6531, p. 69–83, Springer, Berlin, Heidelberg, DOI: 10.1007/978-3-642-18178-8_7, 2010. – *supervised research.*
31. Misoczki, R.; BARRETO, P. S. L. M.: "Compact McEliece Keys from Goppa Codes." In: Workshop on Selected Areas in Cryptography – SAC 2009, Calgary, Canada. Lecture Notes in Computer Science. Heidelberg: Springer, 2009. v. 5867. p. 376–392, DOI: 10.1007/978-3-642-05445-7_24, 2009. – *supervised research.*
32. Naehrig, M.; BARRETO, P. S. L. M.; Schwabe, P.: "On compressible pairings and their computation." In: Progress in Cryptology – Africacrypt 2008, Casablanca, Morocco. Lecture Notes in Computer Science. Heidelberg: Springer, 2008. v. 5023. p. 371–388, DOI: 10.1007/978-3-540-68164-9_25, 2008. – *equal contribution on all aspects.*
33. Deusajute, A. M.; BARRETO, P. S. L. M.: "The SIP Security Enhanced by Using Pairing-assisted Massey-Omura Signcryption." In: X Reunión Española sobre Criptología y Seguridad de la Información – RECSI 2008, 2008, Salamanca, Spain. Anales de la X Reunión Española sobre Criptología y Seguridad de la Información – RECSI 2008, (also available from the IACR ePrint Archive, Report 2008/072), 2008. – *supervised research.*
34. BARRETO, P. S. L. M.; Deusajute, A. M.; Cruz, E; Pereira, G. C. C. F.; Silva, R. R.: "Toward Efficient Certificateless Signcryption from (and without) Bilinear Pairings." In: Proceedings of the 8th Brazilian Symposium on Information and Computer Systems Security – SBSeg 2008, Gramado, Brazil. Brazilian Computer Society (SBC), 2008. – *supervised research.*
35. Simplicio Jr., M. A.; BARRETO, P. S. L. M.; Carvalho, T. C. M. B.; Margi, C. B.; Näslund, M.: "The CURUPIRA-2 Block Cipher for Constrained Platforms: Specification and Benchmarking." In: European Symposium on Research in Computer Security – ESORICS 2008, Málaga, Spain. Proceedings of the 13th European Symposium on Research in Computer Security (ESORICS 2008) and the 8th International Workshop on Privacy in Location-Based Applications (PiLBA 2008), 2008. – *supervised research.*
36. BARRETO, P. S. L. M.; Simplicio Jr., M. A.: "CURUPIRA, a block cipher for constrained platforms." In: Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos – SBRC 2007, 2007, Belém, Brazil. Proceedings of the 25th

Brazilian Symposium on Computer Networks and Distributed Systems, p. 61–74, 2007. – *supervised research.*

37. Ronan, R.; Ó hÉigeartaigh, C.; Murphy, C.; Kerins, T.; BARRETO, P. S. L. M.: “A Reconfigurable Processor for the Cryptographic η_T Pairing in Characteristic 3.” In: International Conference on Information Technology – ITNG 2007, 2007, Las Vegas, USA. Proceedings of the 4th International Conference on Information Technology. p. 11 – 16, DOI: 10.1109/ITNG.2007.19, 2007. – *equal contribution on all aspects.*
38. Gazzoni Filho, D. L.; BARRETO, P. S. L. M.; Rijmen, V.: “The Maelstrom-0 Hash Function.” In: Proceedings of the 6th Brazilian Symposium on Information and Computer Systems Security – SBSeg 2006, Santos, Brazil. Brazilian Computer Society (SBC), 2006. – *supervised research.*
39. Wongtschowski, A.; Ruggiero, W. V.; BARRETO, P. S. L. M.: “Attacking the Java Virtual Machine to Capture Critical User Information.” In: VII Simpósio de Segurança em Informática – SSI 2005, 2005, São José dos Campos, Brazil. Anais SSI 2005, 2005. – *supervised research.*
40. Kerins, T.; Marnane, W.; Popovici, E.; BARRETO, P. S. L. M.: “Efficient hardware for the Tate pairing calculation in characteristic three.” In: Cryptographic Hardware and Embedded Systems – CHES 2005, Edinburgh, UK. Lecture Notes in Computer Science. Heidelberg: Springer, v. 3659. p. 412–426, DOI: 10.1007/11545262_30, 2005. – *equal contribution on all aspects.*
41. BARRETO, P. S. L. M.; Libert, B.; McCullagh, N.; Quisquater, J.-J.: “Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps.” In: Advances in Cryptology – Asiacrypt 2005, Chennai, India. Lecture Notes in Computer Science. Heidelberg: Springer. v. 3788. p. 515–532, DOI: 10.1007/11593447_28, 2005. – *equal contribution on all aspects.*
42. McCullagh, N.; BARRETO, P. S. L. M.: “A New Two-Party Identity-Based Authenticated Key Agreement.” In: Topics in Cryptology – CT-RSA 2005, San Francisco, USA. Lecture Notes in Computer Science. Heidelberg: Springer, v. 3376. p. 262–274, DOI: 10.1007/978-3-540-30574-3_18, 2005. – *equal contribution on all aspects.*
43. BARRETO, P. S. L. M.; Naehrig, M.: “Pairing-Friendly Elliptic Curves of Prime Order.” In: Selected Areas in Cryptography – SAC 2005, Kingston, Canada. Lecture Notes in Computer Science. Heidelberg: Springer, v. 3897. p. 319–331, DOI: 10.1007/11693383_22, 2005. – *equal contribution on all aspects.*
44. BARRETO, P. S. L. M.; Scott, M.: “Compressed Pairings.” In: Advances in Cryptology – Crypto 2004, Santa Barbara, CA. Lecture Notes in Computer Science. Heidelberg: Springer, v. 3152. p. 140–156, DOI: 10.1007/978-3-540-28628-8_9, 2004. – *equal contribution on all aspects.*
45. BARRETO, P. S. L. M.; Lynn, B.; Scott, M.: “On the Selection of Pairing-Friendly Groups.” In: Selected Areas in Cryptography – SAC 2003, Ottawa, Canada. Lecture Notes in Computer Science. Heidelberg: Springer, v. 3006, p. 17–25, DOI: 10.1007/978-3-540-24654-1_2, 2003. – *equal contribution on all aspects.*
46. Nakahara Jr, J.; BARRETO, P. S. L. M.; Preneel, B.; Vandewalle, J.; Kim, H. Y.: “Square Attacks on Reduced-Round PES and IDEA Block Ciphers.” In: 23rd Symposium on Information Theory in the Benelux, 2002, Louvain-la-Neuve (Belgium). Proc. 23rd Symposium on Information Theory in the Benelux. Enschede, The Netherlands: Werkgemeenschap voor Informatie- en

Communicatietheorie. p. 187–195 (also available from the IACR ePrint Archive, Report 2001/068), 2002. – *equal contribution on all aspects.*

47. Daemen, J.; Rijmen, V.; BARRETO, P. S. L. M.: “Rijndael: Beyond the AES.” In: Mikulášská Kryptobesídka 2002, Prague, Czech Republic. Proceedings of the 3rd Annual Czech and Slovak Cryptology Workshop, 2002. – *equal contribution on all aspects.*
48. BARRETO, P. S. L. M.; Kim, H. Y.; Lynn, B.; Scott, M.: “Efficient Algorithms for Pairing-Based Cryptosystems.” In: Advances in Cryptology – Crypto 2002, Santa Barbara. Lecture Notes in Computer Science. Heidelberg: Springer, v. 2442, p. 354–369, DOI: 10.1007/3-540-45708-9_23, 2002. – *equal contribution on all aspects.*
49. BARRETO, P. S. L. M.; Lynn, B.; Scott, M.: “Constructing Elliptic Curves with Prescribed Embedding Degrees.” In: Security in Communication Networks – SCN 2002, Amalfi, Italy. Lecture Notes in Computer Science. Heidelberg: Springer, v. 2576. p. 257–267, DOI: 10.1007/3-540-36413-7_19, 2002. – *equal contribution on all aspects.*
50. BARRETO, P. S. L. M.; Kim, H. Y.; Rijmen, V.: “Toward a Secure Public-Key Blockwise Fragile Authentication Watermarking.” In: IEEE International Conference on Image Processing, Thessaloniki, Greece, Proceedings, v. 2. p. 494–497, DOI: 10.1109/ICIP.2001.958536, 2001. – *equal contribution on all aspects.*
51. BARRETO, P. S. L. M.; Rijmen, V.; Nakahara Jr, J.; Preneel, B.; Vandewalle, J.; Kim, H. Y.: “Improved Square Attacks against Reduced-Round Hierocrypt.” In: Fast Software Encryption – FSE 2001, Yokohama, Japan. Lecture Notes in Computer Science. Heidelberg: Springer. v. 2355. p. 165–173, DOI: 10.1007/3-540-45473-X_14, 2001. – *equal contribution on all aspects.*
52. Kim, H. Y.; BARRETO, P. S. L. M.; “Fast Binary Image Resolution Increasing by k-Nearest Neighbor Learning.” In: IEEE International Conference on Image Processing, Vancouver, BC, Canada. Proceedings, v. 2. p. 327–330, DOI: 10.1109/ICIP.2000.899376, 2000. – *equal contribution on all aspects.*
53. BARRETO, P. S. L. M.; Kim, H. Y.; Rijmen, V.: “Um Modo de Operação de Funções de Hashing para Localizar Alterações em Dados Digitalmente Assinados” (in Portuguese). In: Simpósio Brasileiro de Telecomunicações (SBrT 2000), Gramado, Rio Grande do Sul, Brazil. Proceedings of the Brazilian Symposium on Telecommunications (SBrT 2000). – *equal contribution on all aspects.*
54. BARRETO, P. S. L. M.; Rijmen, V.: “The Anubis Block Cipher.” In: 1st Open NESSIE Workshop, 2000, Leuven (Belgium). Proceedings of the 1st Open NESSIE Workshop. – *equal contribution on all aspects.*
55. BARRETO, P. S. L. M.; Rijmen, V.: “The Khazad Legacy-Level Block Cipher.” In: 1st Open NESSIE Workshop, 2000, Leuven (Belgium). Proceedings of the 1st Open NESSIE Workshop. – *equal contribution on all aspects.*
56. BARRETO, P. S. L. M.; Rijmen, V.: “The Whirlpool Hashing Function.” In: 1st Open NESSIE Workshop, 2000, Leuven (Belgium). Proceedings of the 1st Open NESSIE Workshop. – *equal contribution on all aspects.*
57. BARRETO, P. S. L. M.; Kim, H. Y.: “Pitfalls in Public Key Watermarking.” In: Brazilian Symposium on Computer Graphics and Image Processing (Sibgrapi 1999), Campinas, São Paulo, Brazil. Proceedings. p. 241–242, DOI: 10.1109/SIBGRA.1999.805730, 1999.

Books and book chapters

1. BARRETO, P. S. L. M.; Biasi, F. P.; Dahab, R.; López-Hernández, J. C.; Morais, E. M.; Oliveira, A. D. S.; Pereira, G. C. C. F. ; Ricardini, J. E.: A Panorama of Post-quantum Cryptography. In: Koç, Çetin Kaya. (Org.). *Open Problems in Mathematics and Computational Science*. Springer, p. 387–439, DOI: 10.1007/978-3-319-10683-0_16, 2014. – *equal contribution on all aspects.*
2. van Tilborg, H. C. A.; Jajodia, S.; BARRETO, P. S. L. M.; Rijmen, V.: Whirlpool. In: van Tilborg, H. C. A.; Jajodia, S. (Eds.). *Encyclopedia of Cryptography and Security* 2nd Edition. Springer, p. 1384–1385, DOI: 10.1007/978-1-4419-5906-5_626, 2011. – *equal contribution on all aspects.*
3. Libert, B.; Quisquater, J.-J.; BARRETO, P. S. L. M.; McCullagh, N.; 2010: Practical signcryption schemes based on the Diffie-Hellman problem. In: Zheng, Y.; Dent, A. W. (Eds.). Practical Signcryption. Springer, p. 57–70, DOI: 10.1007/978-3-540-89411-7_4, 2010. – *equal contribution on all aspects.*
4. Libert, B.; Quisquater, J.-J.; BARRETO, P. S. L. M.; McCullagh, N.; 2010: Practical signcryption schemes based on bilinear maps. In: Zheng, Y.; Dent, A. W. (Eds.). Practical Signcryption. Springer, p. 71–98, DOI: 10.1007/978-3-540-89411-7_5, 2010. – *equal contribution on all aspects.*
5. Abdalla, M.; BARRETO, P. S. L. M. (Eds.). Progress in Cryptology – LATINCRYPT 2010. Berlin/Heidelberg: Springer, DOI: 10.1007/978-3-642-14712-8, 2010. 322 p. – *editing as program co-Chair.*
6. Avanzi, R.; BARRETO, P. S. L. M.; Gaudry, P.; Scheidler, R.; Thériault, N. (Eds.). Advances in Mathematics of Communications – Special Issue – Conference on Hyperelliptic Curves, Discrete Logarithms, Encryption (CHiLE 2009). Springfield, USA: American Institute of Mathematical Sciences, v. 4, n. 2, 305 p., DOI: 10.3934/amc.2010.4.2i, 2010 – *equal contribution on all aspects.*
7. Margi, C. B.; Simplício Jr., M. A.; BARRETO, P. S. L. M.; Carvalho, T. C. M. B.: “Segurança em Redes de Sensores sem Fio.” In: Santin, A.; Nunes, R. C.; Dahab, R. (Eds.). Minicursos: SBSeg 2009, Brazilian Computer Society (SBC), v. 1, p. 149–194, 2009. – *equal contribution on all aspects.*
8. Kim, H. Y.; Pamboukian, S. V. D.; BARRETO, P. S. L. M.; 2008: Authentication Watermarkings for Binary Images. In: Chang-Tsun Li. (Org.). Multimedia Forensics and Security: IGI Global. – *equal contribution on all aspects.*
9. BARRETO, P. S. L. M.; Rijmen, V.: Dedicated Hash-Function 7 (Whirlpool). In: ISO/IEC. (Org.). ISO/IEC 10118-3:2004: Information technology Security techniques Hash-functions Part 3: Dedicated hash-functions. Geneva: International Organization for Standardization (ISO), p. 19–22. – *equal contribution on all aspects.*

Manuscripts and work in progress

1. BARRETO, P. S. L. M.; Scott, M.: “Pairing-Friendly Elliptic Curves for zk-SNARK Applications,” – work in progress, 2022 – *equal contribution on all aspects*.
2. BARRETO, P. S. L. M.; Ricardini, J. E.; Simplicio Jr., M. A.; Patil, H. K.: “qSCMS: Post-quantum certificate provisioning process for V2X.” Available

from IACR Cryptology ePrint Archive, Report 2018/1247. – *equal contribution on all aspects.*

3. BARRETO, P. S. L. M.; David, B.; R. Dowsley; Morozov, K.; Nascimento, A. C.: “A framework for efficient adaptively secure composable oblivious transfer in the ROM,” (joint work with UW Tacoma faculty). Available from IACR Cryptology ePrint Archive, Report 2017/993. – *equal contribution on all aspects.*

Other publications

1. BARRETO, P. S. L. M.; Elliott, E.: “Improved signcryption and broadcast signcryption with detachable signatures,” – unpublished manuscript, 2020. – *supervised research.*
2. BARRETO, P. S. L. M.; Linardopoulou, T.: “Efficient algorithms for the NIST PQC candidate NTRU cryptosystem,” – unpublished manuscript, 2020. – *supervised research.*
3. BARRETO, P. S. L. M.; Longa, P.; Naehrig, M.; Ricardini, J. E.; Zanon, G.: “Sharper Ring-LWE Signatures,” Cryptology ePrint Archive, Report 2016/1026. – *equal contribution on all aspects.*
4. BARRETO, P. S. L. M., M. Naehrig, “Elliptic curve generation – BN curves,” contribution to the ISO/IEC 15946-5 standard. Geneva, Switzerland: ISO/IEC, 2007. – *equal contribution on all aspects.*
5. BARRETO, P. S. L. M., B. Libert, N. McCullagh, J.-J. Quisquater, “Efficient and secure identity-based signatures and signcryption from bilinear maps,” contribution to the P1363.3 working group of the IEEE Standards Association. New Jersey, USA: IEEE, 2006. – *equal contribution on all aspects.*
6. BARRETO, P. S. L. M., M. Naehrig, “Pairing-Friendly Elliptic Curves of Prime Order with Embedding Degree 12,” contribution to the P1363.3 Working Group of the IEEE Standards Association. New Jersey, USA: IEEE, 2006. – *equal contribution on all aspects.*
7. V. Rijmen, BARRETO, P. S. L. M., “The Khazad Block Cipher,” *The Perl Journal* v. 7, p. 5, 2003. – *equal contribution on all aspects.*
8. BARRETO, P. S. L. M.: “An Efficient LALR(1) and LR(1) Lookahead Set Algorithm,’’ – unpublished manuscript, 1989. – *individual research.*

Invited talks

1. BARRETO, P. S. L. M.: “Post-Quantum Cryptography from 2007 to 2020” (in Portuguese: “Criptografia Pós-Quântica – de 2007 a 2020”), Brazilian Symposium on Information and Computational Systems Security (SBSeg 2020), Petrópolis, Rio de Janeiro, Brazil (held virtually); http://sbseg.sbc.org.br/2020/en/programacao_en.html, 2020.
2. BARRETO, P. S. L. M.: “Post-Quantum Cryptography – Classical Security in the Presence of Quantum Computers” (in Portuguese: “Criptografia Pós-Quântica – Segurança Clássica na Presença de Computadores Quânticos”), Brazilian Navy

Symposium on Operational Research and Logistics (SPOLM 2019), Rio de Janeiro, Brazil, 2019.

3. BARRETO, P. S. L. M.: "Supersingular Isogeny-Based Cryptography – Overview and Research Challenges," OSU School of EECS Seminars in Computer Science, Corvallis, OR, 2019.
4. BARRETO, P. S. L. M.: "Faster key compression for isogeny-based cryptosystems," Séminaires en informatique de l'École Polytechnique, Centre de Recherche INRIA Saclay, Paris-Palaiseau, France, 2018.
5. BARRETO, P. S. L. M.: "Toward Practical Code-Based Cryptography," Code-Based Cryptography Workshop (CBC 2018), Florida Atlantic University, Davie, FL; http://www.math.fau.edu/codebasedcryptoworkshop2018/, 2018.
6. BARRETO, P. S. L. M.: "Toward a Post-Quantum PKI," Center for Data Science Seminar Series, University of Washington Tacoma, Tacoma, WA, 2016.
7. BARRETO, P. S. L. M.: "Introduction to Code-Based Cryptography," SP Coding and Information School, University of Campinas, Campinas, São Paulo, Brazil, 2015.
8. BARRETO, P. S. L. M.: "How Deployable is Code-Based Cryptography?" Microsoft Research Seminars, Microsoft Campus, Redmond, WA, 2014.
9. BARRETO, P. S. L. M.: "A Panorama of Post-Quantum Cryptography," Open Problems in Mathematical and Computational Sciences Conference, Sait Salim Pasha Palace, Istanbul, Turkey, 2013.
10. BARRETO, P. S. L. M.: "How to Write a Research Paper" (in Portuguese: "Como Escrever um Artigo de Pesquisa"), Graduate Seminars in Electrical and Computer Engineering, Escola Politécnica, University of São Paulo, São Paulo, Brazil, 2013.
11. BARRETO, P. S. L. M.: "The Realm of the Pairings," Conference on Selected Ares in Cryptography (SAC 2013) – Distinguished Lecture; Simon Fraser University; Burnaby, BC, Canada, 2013.
12. BARRETO, P. S. L. M.: "Code-Based Cryptography," São Paulo Advanced School of Cryptography (ASCrypto 2013), Florianópolis, Santa Catarina, Brazil, 2011.
13. BARRETO, P. S. L. M.: "Can code-based keys and cryptograms get smaller than their RSA counterparts?" Post-Quantum Cryptography and Quantum Algorithms Workshop, Universiteit Leiden Lorentz Center, Leiden, The Netherlands, http://www.lorentzcenter.nl/lc/web/2012/519/program.php3?wsid=519&venue=Oort, 2012.
14. BARRETO, P. S. L. M.: "Pairing-Based Cryptography," São Paulo Advanced School of Cryptography (ASCrypto 2011), Atibaia, São Paulo, Brazil, 2011.
15. BARRETO, P. S. L. M.: "Efficient Implementation of Post-Quantum Cryptosystems Based on Coding Theory" (in Portuguese: "Implementação eficiente de criptossistemas pós-quânticos baseados em teoria dos códigos"), Workshop on Coding Theory and Cryptography, Santo André, São Paulo, Brazil, 2010.
16. BARRETO, P. S. L. M.: "Post-Quantum Cryptography: Introduction and Trends," Joint NIST/JQI and University of Maryland Quantum Information Workshop, Washington DC, 2010.
17. BARRETO, P. S. L. M.: "A Simple Introduction to Syndrome-Decoding-Based Cryptography," Dublin City University Seminars on Information Security and Cryptography, Dublin, Ireland, 2009.

18. BARRETO, P. S. L. M.: “Dyadic Goppa codes for code-based cryptosystems,” Coding-Based Cryptography Workshop, INRIA Paris-Rocquencourt, France, 2009.
19. BARRETO, P. S. L. M.: “How to obtain short McEliece keys using Goppa codes,” Claude Shannon Institute Workshop on Coding and Cryptography, University College Cork , Cork, Ireland, 2009.
20. BARRETO, P. S. L. M.: “Pairings in Real Life,” Workshop on Pairings in Arithmetic Geometry and Cryptography, Universität Duisburg-Essen, Essen, Germany, 2009.
21. BARRETO, P. S. L. M.: “Post-quantum cryptosystems based on coding theory: overview and recent developments,” ECRYPT Western European Workshop on Research in Cryptology (WEWoRC 2009), Technische Universität Graz, Graz, Austria, 2009.
22. BARRETO, P. S. L. M.: “Recent Trends in Post-Quantum Cryptography,” Claude Shannon Institute and University College Dublin Irish Cryptography Day, Dublin, Ireland, 2009.
23. BARRETO, P. S. L. M.: “Syndrome-Based Post-Quantum Cryptography,” Royal Holloway University of London Seminars on Cryptology, Royal Holloway University of London, Egham, UK, 2009.
24. BARRETO, P. S. L. M.: “Post-Quantum Cryptography” (in Spanish: “Criptografía post-cuántica”), Congreso Iberoamericano de Seguridad Informática (CIBSI 2007), conferencia magistral invitada, Universidad Nacional del Centro de la Provincia de Buenos Aires, Mar del Plata, Argentina, 2007.
25. BARRETO, P. S. L. M.: “Post-Quantum Cryptography: An Overview,” Workshop on Cryptographic Algorithms and Protocols (WCAP 2007), Brazilian Computer Society, Federal University of Rio de Janeiro, Rio de Janeiro, Brazil, 2007.
26. BARRETO, P. S. L. M.: “Topics in Cryptanalysis” (in Portuguese: “Tópicos em Criptoanálise”), Workshop on Complex Systems and Cognition, Santo André, São Paulo, Brazil, 2007.
27. BARRETO, P. S. L. M.: “The Hash Function Crisis” (in Portuguese: “A Crise das Funções de Hash”), Brazilian Symposium on Information Security (SSI 2005), Aerospace Technical Center, São José dos Campos, São Paulo, Brazil, 2005.
28. BARRETO, P. S. L. M.: “Pairing-Based Cryptography,” Workshop on Cryptographic Algorithms and Protocols (WCAP 2005), Brazilian Computer Society, Federal University of Santa Catarina, Florianópolis, Santa Catarina, Brazil, 2005.
29. BARRETO, P. S. L. M.: “Pairing-Friendly Curves of Prime and Near-Prime Order,” International Workshop on Pairings in Cryptography (PiC 2005), ECRYPT – European Network of Excellence for Cryptology, Dublin City University, Dublin, Ireland, 2005.
30. BARRETO, P. S. L. M.: “Cryptographic Algorithms – International Panorama” (in Portuguese: “Algoritmos Criptográficos – Panorama Internacional”), Brazilian Presidential Office Seminar on Cryptography (in Portuguese: Seminário sobre Criptografia no Palácio do Planalto), Planalto Palace, Brasília, Brazil, 2004.
31. BARRETO, P. S. L. M.: “Cryptography in the Protection of Information Technology: Trends and Challenges” (in Portuguese: “Criptografia na Proteção da TI: Tendências e Desafios”), Brazilian Navy Symposium on Information Technology (INFORMAR 2004), Rio de Janeiro, Brazil, 2004.

32. BARRETO, P. S. L. M.: “Cryptographic Applications of Bilinear Pairings – A Hands-On Introduction,” ECRYPT Summer School on Elliptic Curves in Cryptography, Ruhr-Universität Bochum, Bochum, Germany, 2004.
33. BARRETO, P. S. L. M.: “The Well-Tempered Pairing,” Workshop on Elliptic Curve Cryptography (ECC 2004), Ruhr-Universität Bochum, Bochum, Germany, 2004.

Service in program committees

I am a member of the Steering Committee of the Latincrypt Series of International Conferences on Cryptology and Information Security in Latin America since its inception in 2010, when I co-chaired this conference’s first installment. This includes the ASCrypto series of advanced schools in cryptography, which alternates yearly with the Latincrypt conference.

I have served or am currently serving on the Program Committees of the following conferences in the indicated roles:

1. CT-RSA 2023 – Cryptographer’s Track at the RSA Conference (program committee member).
2. CT-RSA 2022 – Cryptographer’s Track at the RSA Conference (program committee member).
3. Eurocrypt 2022 – International Conference on the Theory and Applications of Cryptographic Techniques (program committee member).
4. SAC 2022 – Conference on Selected Areas of Cryptography (program committee member).
5. SBSeg 2022 – Brazilian Symposium on Information and Computational Systems Security (program committee member).
6. CT-RSA 2021 – Cryptographer’s Track at the RSA Conference (program committee member).
7. Indocrypt 2021 – International Conference on Cryptology in India (program committee member).
8. PKC 2021 – International Conference on Practice and Theory of Public-Key Cryptography (program committee member).
9. SAC 2021 – Conference on Selected Areas of Cryptography (program committee member).
10. SBSeg 2021 – Brazilian Symposium on Information and Computational Systems Security (program committee member).
11. Asiacrypt 2020 – International Conference on the Theory and Application of Cryptology and Information Security (program committee member).
12. CT-RSA 2020 – Cryptographer’s Track at the RSA Conference (program committee member).
13. ECC 2020 – Elliptic curve cryptography workshop (program committee member).
14. SAC 2020 – Conference on Selected Areas of Cryptography (program committee member).

15. Asiacrypt 2019 – International Conference on the Theory and Application of Cryptology and Information Security (program committee member).
16. CBC 2019 – Workshop on Code-Based Cryptography (program committee member).
17. CRYPTO 2019 – International Cryptology Conference (reviewer).
18. Eurocrypt 2019 – International Conference on the Theory and Applications of Cryptographic Techniques (program committee member).
19. Latincrypt 2019 – International Conference on Cryptology and Information Security in Latin America (program committee member).
20. PQCrypto 2019 – Post Quantum Cryptography Conference (reviewer).
21. SAC 2019 – Conference on Selected Areas of Cryptography (program committee member).
22. ACISP 2018 – Australasian Conference on Information Security and Privacy (program committee member).
23. CRYPTO 2018 – International Cryptology Conference (reviewer).
24. Eurocrypt 2018 – International Conference on the Theory and Applications of Cryptographic Techniques (program committee member).
25. ISC 2018 – Information Security Conference (program committee member).
26. PQCrypto 2018 – Post Quantum Cryptography Conference (reviewer).
27. SAC 2018 – Conference on Selected Areas of Cryptography (program committee member).
28. CBC 2017 – Code-Based Cryptography workshop 2017 (program committee member).
29. Latincrypt 2017 – International Conference on Cryptology and Information Security in Latin America (program committee member).
30. PQCrypto 2017 – Post Quantum Cryptography Conference (reviewer).
31. SAC 2017 – Conference on Selected Areas of Cryptography (program committee member).
32. CRYPTO 2016 – International Cryptology Conference (reviewer).
33. ECC 2016 – Workshop on Elliptic Curve Cryptography (program committee member).
34. FC 2016 – Financial Cryptography and Data Security Conference (program committee member).
35. ICITS 2016 – International Conference on Information Theoretic Security (co-Chair).
36. PKC 2016 – International Conference on Practice and Theory of Public-Key Cryptography (program committee member).
37. SAC 2016 – Conference on Selected Areas of Cryptography (program committee member).
38. ACISP 2015 – Australasian Conference on Information Security and Privacy (program committee member).
39. CRYPTO 2015 – International Cryptology Conference (program committee member).
40. ECC 2015 – Workshop on Elliptic Curve Cryptography (program committee member).
41. ICITS 2015 – International Conference on Information Theoretic Security (program committee member).

42. Latincrypt 2015 – International Conference on Cryptology and Information Security in Latin America (program committee member).
43. SAC 2015 – Conference on Selected Areas of Cryptography (program committee member).
44. SECITC 2015 – International Conference on Security for Information Technology and Communications (program committee member).
45. Asiacrypt 2014 – International Conference on the Theory and Application of Cryptology and Information Security (program committee member).
46. Latincrypt 2014 – International Conference on Cryptology and Information Security in Latin America (program committee member).
47. LightSec 2014 – International Workshop on Lightweight Cryptography for Security & Privacy (program committee member).
48. PKC 2014 – International Conference on Practice and Theory of Public-Key Cryptography (program committee member).
49. PQCrypto 2014 – Post Quantum Cryptography Conference (program committee member).
50. ProvSec 2014 – International Conference on Provable and Practical Security (program committee member).
51. SBSeg 2014 – Brazilian Symposium on Information and Computational Systems Security (program committee member).
52. ACISP 2013– Australasian Conference on Information Security and Privacy (program committee member).
53. CANS 2013 – International Conference on Cryptology And Network Security (program committee member).
54. LightSec 2013 – International Workshop on Lightweight Cryptography for Security & Privacy (program committee member).
55. Pairing 2013 – International Conference on Pairing-Based Cryptography (program committee member).
56. PQCrypto 2013 – Post Quantum Cryptography Conference (program committee member).
57. SAC 2013 – Conference on Selected Areas of Cryptography (program committee member).
58. SBSeg 2013 – Brazilian Symposium on Information and Computational Systems Security (program committee member).
59. ACISP 2012– Australasian Conference on Information Security and Privacy (program committee member).
60. ACNS 2012 – International Conference on Applied Cryptography and Network Security (program committee member).
61. CHES 2012 – Conference on Cryptographic Hardware and Embedded Systems (program committee member).
62. Latincrypt 2012 – International Conference on Cryptology and Information Security in Latin America (program committee member).
63. Pairing 2012 – International Conference on Pairing-Based Cryptography (program committee member).
64. SBSeg 2012 – Brazilian Symposium on Information and Computational Systems Security (program committee member).

65. CHES 2011 – Conference on Cryptographic Hardware and Embedded Systems (program committee member).
66. CRYPTO 2011 – International Cryptology Conference (program committee member).
67. LightSec 2011 – International Workshop on Lightweight Cryptography for Security & Privacy (program committee member).
68. PQCrypto 2011 – Post Quantum Cryptography Conference (program committee member).
69. SBSeg 2011 – Brazilian Symposium on Information and Computational Systems Security (program committee member).
70. Africacrypt 2010 – International Conference on Cryptology in Africa (program committee member).
71. Latincrypt 2010 – International Conference on Cryptology and Information Security in Latin America (program chair).
72. Pairing 2010 – International Conference on Pairing-Based Cryptography (program committee member).
73. PQCrypto 2010 – Post Quantum Cryptography Conference (program committee member).
74. SAC 2010 – Conference on Selected Areas of Cryptography (program committee member).
75. SBSeg 2010 – Brazilian Symposium on Information and Computational Systems Security (program committee member).
76. Africacrypt 2009 – International Conference on Cryptology in Africa (program committee member).
77. CHiLE 2009 – Conference on Hyperelliptic curves, discrete Logarithms, Encryption (program committee member).
78. Eurocrypt 2009 – International Conference on the Theory and Applications of Cryptographic Techniques (program committee member).
79. ISC 2009 – International Conference on Information Security (program committee member).
80. Pairing 2009 – International Conference on Pairing-Based Cryptography (program committee member).
81. SAC 2009 – Conference on Selected Areas of Cryptography (program committee member).
82. SBSeg 2009 – Brazilian Symposium on Information and Computational Systems Security (program committee member).
83. Indocrypt 2008 – International Conference on Cryptology in India (program committee member).
84. Pairing 2008 – International Conference on Pairing-Based Cryptography (program committee member).
85. SAC 2008 – Conference on Selected Areas of Cryptography (program committee member).
86. SBSeg 2008 – Brazilian Symposium on Information and Computational Systems Security (program committee member).
87. ISC 2007 – International Conference on Information Security (program committee member).

88. Pairing 2007 – International Conference on Pairing-Based Cryptography (program committee member).
89. SBSeg 2007 – Brazilian Symposium on Information and Computational Systems Security (program committee member).
90. Asiacrypt 2006 – International Conference on the Theory and Application of Cryptology and Information Security (program committee member)
91. Indocrypt 2006 – International Conference on Cryptology in India (program committee member).
92. PKC 2006 – International Conference on Practice and Theory of Public-Key Cryptography (program committee member).
93. SBSeg 2006 – Brazilian Symposium on Information and Computational Systems Security (program committee member).
94. Asiacrypt 2005 – International Conference on the Theory and Application of Cryptology and Information Security (program committee member).
95. CT-RSA 2005 – Cryptographer's Track at the RSA Conference (program committee member)
96. SBSeg 2005 – Brazilian Symposium on Information and Computational Systems Security (program committee member).

Contributions to technology standards

1. The Whirlpool hash function: ISO/IEC 10118-4.
2. The BLMQ digital signature and signcryption scheme: ISO-IEC 15946-5, IEEE 1363.3-2013.
3. The Barreto-Naehrig (BN) and Barreto-Lynn-Scott (BLS) families of pairing-friendly elliptic curves: ISO-IEC 15946-5, IEEE 1363.3-2013.

Projects coordinated by the author (academic scope)

1. FAPESP theme project "Information security and reliability: theory and applications," 2014. Funding amount: R$ 837,311.00 plus US$ 11,000.00 (joint project with the University of Campinas).
2. Universal CNPq 2011. Funding amount: R$ 49,980.00
3. Universal CNPq 2007. Funding amount: R$ 20,000.00

Participation in projects (academic scope)

1. FAPESP theme project "Information security and reliability: theory and applications – second phase," 2019. (joint project with the University of São Paulo and the University of Campinas).
2. University Global Partnership Network project "Development and Analysis of Post-quantum Cryptosystems and Their Applications," 2018. Funding amount:

US$ 30,000.00 (joint project with researchers from the University of Wollongong, University of Surrey, and University of São Paulo).

Projects coordinated with industry

1. Intel Strategic Research Alliance (ISRA) project "Energy-efficient Security for SoC Devices – Asymmetric Cryptography for Embedded Systems," 2012 (original timeframe: 2013–2015, extended in 2013 as a joint Intel & Brazilian National Council for Scientific and Technological Development (CNPq) project for the timeframe 2014–2016 with doubled funding). Funding amount: US$ 100,000.00 per year 2013–2014, US$ 200,000.00 per year 2015–2016.
2. Scopus Tecnologia S.A. research project "Security framework for digital cash," timeframe 2009–2015 (renewed yearly). Funding amount: R$ 160.000,00 per year.
3. Cisco Research grant 2011-050 "Alternate Public Key Cryptosystems," 2011. Funding amount: US$ 100,000.00

Participation as consultant in other projects with industry and/or government

1. LG Electronics: Security protocols for vehicular communications (2018)
2. Ericsson Research: Personalized mobile health solutions – security aspects (2012-2013)
3. National Instruments: Security Framework for LabVIEW™ (2011)
4. Scopus Tecnologia S/A: Lightweight PKI for Mobile Platforms (2009-2012)
5. Unibanco S/A: IT Security Concepts for Financial Applications (2006)
6. Ericsson Research: Lightweight Ciphers for Wireless Sensor Networks (2007-2010)
7. MBA course, several companies: Fundamentals of Information Security (2002-2008).
8. Government of the State of São Paulo (Brazil): tax payment digital authentication system (2000-2003).

Co-author list

1. Abdalla, Michel
2. Aguilar-Melchor, Carlos
3. Akleylek, Sedat
4. Albertini, Bruno C.
5. Alkim, Erdem
6. Almeida, Leonardo C.
7. Andrade, Ewerton R.
8. Aragon, Nicolas
9. Aranha, Diego F.

10. Avanzi, Roberto

11. Banegas, Gustavo
12. Barbier, Morgan
13. Barbuda, Pedro A. F. F. S.
14. Barguil, João M. M.
15. Benits, Waldyr
16. Bettaieb, Slim
17. Biasi, Felipe P.
18. Bidoux, Loïc
19. Bindel, Nina
20. Blazy, Olivier
21. Boidje, Brice O.
22. Buchmann, Johannes

23. Carvalho, Tereza C. M. B.
24. Cayrel, Pierre-Louis
25. Chu, Peter
26. Costa, Carlos H. A.
27. Costello, Craig

28. David, Bernardo
29. Deneuville, Jean-Christophe
30. Dione, Gilbert N.
31. Doliskani, Javad
32. Dowsley, Rafael

33. Eaton, Edward
34. Elliott, Edgar

35. Farias, Luckas A.
36. Furuie, Sergio S.

37. Gaborit, Philippe
38. Gaj, Kris
39. Galbraith, Steven D.
40. Gaudry, Pierrick
41. Gazzoni Filho, Décio L.
42. Ghosh, Santosh
43. Gold, Richard
44. Gueron, Shay
45. Gueye, Cheikh T.
46. Güneysu, Tim
47. Gutoski, Gus

48. Haeussler, Richard

49. Januário, Guilherme C.

50. Kerins, Tim

51. Kim, Haeyong
52. Klamti, Jean B.
53. Kobayashi, Luiz O. M.
54. Krämer, Juliane

55. Libert, Benoît
56. Linardopoulou, Tatiana
57. Lindner, Richard
58. Lino, Renan Y.
59. Longa, Patrick
60. Lynn, Ben Y. S.

61. Maia, Ricardo J. M.
62. Massolino, Pedro M. C
63. Margi, Cíntia B.
64. Marnane, William P.
65. McCullagh, Noel
66. Misoczki, Rafael
67. Moreira, José E.
68. Morozov, Kirill.
69. Murphy, Colin C.

70. Naehrig, Michael
71. Näslund, Mats
72. Nakahara, Jorge
73. Nascimento, Anderson C.
74. N’diaye, Ousmane
75. Nguyen, Duc T.
76. Niebuhr, Robert
77. Nikov, Ventzislav
78. Nikova, Svetla

79. Oliveira, Bruno T.
80. Oliveira, Gláucio A.
81. Ó hÉigeartaigh, Colm

82. Pamboukian, Sergio V. D.
83. Patil, Harsh K.
84. Pereira, Geovandro C. C. F.
85. Persichetti, Edoardo
86. Polat, Harun
87. Popovici, Emanuel M.
88. Possignolo, Rafael T.
89. Preneel, Bart
90. Puodzius, Cassius

91. Quisquater, Jean-Jacques

92. Reich, Devin D.
93. Ricardini, Jefferson E.

94. Richter-Brockmann, Jan
95. Rijmen, Vincent
96. Ronan, Robert
97. Ruggiero, Wilson V.

98. Santini, Paolo
99. Santos, Mateus A. S.
100. Santos, Paulo C. F.
101. Scheidler, Renate
102. Schwabe, Peter
103. Sendrier, Nicolas
104. Scott, Michael P. J.
105. Simplício, Marcos A.
106. Sousa, Gustavo T.

107. Thériault, Nicolas
108. Tillich, Jean-Pierre
109. Tischhauser, Elmar

110. Vandewalle, Joos P. L.
111. Vasseur, Valentin
112. Voloch, José F.

113. Zanon, Gustavo H. M.
114. Zémor, Gilles

□