Curriculum Vitæ

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

Spring 2016

I was born in the city of Salvador, capital of the State of Bahia, Brazil. I obtained my BSc in Physics in 1987, received my Ph.D. degree in Engineering in 2003 and my Habilitation in Computer Engineering in 2011, all at the University of São Paulo. I worked at Unisys Brazil Ltd and Scopus Tecnologia S/A as systems software analyst and developer, and then as chief cryptographer. I joined the faculty at the Department of Computer and Digital Systems Engineering, Escola Politécnica, University of São Paulo in 2004 as Assistant Professor, and became Associate Professor there in 2011. I finally joined the faculty as Assistant Professor at the Institute of Technology, University of Seattle Tacoma, on September 1st, 2015.

I am one of the designers of the Whirlpool hash function (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 signcrytion methods), and the construction of pairing-friendly elliptic curves (e.g. the BN and BLS families of elliptic curves), many of them adopted in ISO-IEC 15946-5. More recently I have been working on efficient algorithms for quantum-resistant (also called post-quantum) cryptosystems, including code-based, lattice-based, hash-based and multivariate schemes

I have served in 23 PhD defense committees (7 of which outside Brazil) and 27 MSc defense committees since 2005. I supervised to completion 3 PhD theses (since 2010) and 8 MSc theses (since 2008). I also served in the program committees of almost 60 conferences over the past ten years, 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. Furthermore, I am an Associated Editor of the Journal of Cryptographic Engineering (since 2011), IEEE Transactions on Computers (since 2015), and IET Information Security (since 2015).

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 also granted:

- Best Paper Awards at the 6th Brazilian Symposium on Information and Computer Systems Security (SBSeg 2006).
- Best Paper Award at the 6th Brazilian Symposium on Information and Computer Systems Security (SBSeg 2006).
- Best Paper Award at the 25th Brazilian Symposium on Computer Networks and Distributed Systems (SBRC 2007).
- 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 MSc Thesis Supervision Award at the 10th Brazilian Symposium on Information and Computer Systems Security (SBSeg 2010).
- Best PhD Thesis Supervision Award at the 10th Brazilian Symposium on Information and Computer Systems Security (SBSeg 2010).
- Honor Mention for PhD Thesis Supervision in Engineering at the Brazilian national level, CAPES Foundation, 2011.

I was 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 also granted the E. T. S. Walton Award by the Science Foundation Ireland (SFI) under grant 07/W.1/I1824.

I have given over 20 invited talks, and I was chosen as Distinguished Lecturer at the 20th anniversary Selected Areas in Cryptography conference (2013).

My Hirsch Index (*h*-index) is 15 according to the Web of Science; 17 according to Scopus, and 28 according to Google Scholar.

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 the past 10 years, I have been teaching 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 (60 hours, undergrad level)
- Computer Networks (undergrad level)

I am currently teaching or schedule to teach in the next quarters the following courses at the University of Washington Tacoma:

- Advanced Algorithms (Winter and Summer 2016; grad level)
- Design and Analysis of Algorithms (Autumn 2015 and 2016, Winter and Spring 2016 and 2017; undergrad level)
- Compiler Construction (Spring 2016 and 2017; undergrad level)
- Undergraduate Seminar in CSS (Summer 2016, undergrad level)

I am also a member of the MSc in Computer Science program committee at the Institute of Technology of the University of Washington Tacoma. In this context, I am working to create the new course on Post-Quantum Cryptography (to be offered for the first time in 2016). I am also collaborating 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
- Efficient algorithms for pairing-based cryptosystems
- Identity-based key agreement schemes, digital signatures and signcryption from bilinear pairings
- Construction of pairing-friendly elliptic curves
- Efficient and side-channel-resistant implementation of pairings and elliptic curve cryptography
- Code-based encryption
- Hash-based digital signatures
- Lattice-based and homomorphic cryptosystems

Journal papers:

1. 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, 2016, to appear. DOI: 10.1109/TC.2016.2516011.
2. Pereira, G. C. C. F.; Puodzius, C. O.; BARRETO, P. S. L. M.: “Shorter Hash-Based Signatures.” The Journal of Systems and Software, 2015, v. 116, p. 95-100.

3. 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, 2015.
4. 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, 2015.
5. 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, 2015.
6. 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, 2014.
7. 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, 2014.
8. 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, 2013.
9. 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, 2013.
10. 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, 2013.
11. 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, 2012.
12. 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, 2011.
13. 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, 2011.
14. 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, 2010.
15. 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, 2010.
16. 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, 2010.
17. 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* **2(2)**, 165–180, Wiley Interscience, 2009.
18. 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, 2009.

19. 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.
20. Rijmen, V.; BARRETO, P. S. L. M.; Gazzoni Filho, D. L.: “Rotation symmetry in algebraically generated cryptographic substitution tables”, *Information Processing Letters* **106**, 246–250, 2008.
21. BARRETO, P. S. L. M.; Galbraith, S.; Ó hÉigeartaigh, C.; Scott, M.: “Efficient Pairing Computation on Supersingular Abelian Varieties.” *Designs, Codes and Cryptography* **42**, 239–271, 2007.
22. 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* **1**, 79–88, 2007.
23. 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, 2007.
24. Scott, M., BARRETO, P. S. L. M.: “Generating more MNT elliptic curves.” *Designs, Codes and Cryptography* **38**, 209–217, 2006.
25. BARRETO, P. S. L. M.; Voloch, F.: “Efficient Computation of Roots in Finite Fields.” *Designs, Codes and Cryptography* **39**, 275–280, 2006.
26. Kerins, T.; Marnane, W.; Popovici, E.; BARRETO, P. S. L. M.: “Hardware Accelerators for Pairing Based Cryptosystems. *IEE Proceedings on Information Security* **152**, 47–56, 2005.
27. 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* **2**, 19–28, 2005.
28. BARRETO, P. S. L. M.; Lynn, B.; Scott, M.: “Efficient Implementation of Pairing-Based Cryptosystems.” *Journal of Cryptology* **17**, 321–334, 2004.
29. BARRETO, P. S. L. M.: “Aspecto e comprometimento: nota sobre antropologia e gramática” (in Portuguese), *Videtur* 28, 33 – 34.
30. 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* **149**, 57–62, 2002.

Conference papers:

1. 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, 2015.
2. 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), 2015, Foz do Iguaçu. SBESC 2015 Proceedings, 2015.
3. 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.
4. 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, 2014.
5. 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, 2013.
6. Aranha, D. F.; Longa, P.; BARRETO, P. S. L. M.; Ricardini, J. E.; 2014: The Realm of the Pairings. In: Selected Areas in Cryptography – SAC 2013, Lecture Notes in Computer Sience, Heidelberg: Springer, 2014. v. 8282. p. 3-25.
7. 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, 2012. p. 62-71.
8. 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, 2011, p. 2681-2685.
9. 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, 2011.
10. 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, 2011.
11. 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.; 2010: Impact of Operating Systems on Wireless Sensor Networks (Security) Applications and Testbeds. In: International Conference on Computer Communication Networks (ICCCN 2010) / IEEE International Workshop on Wireless Mesh and Ad Hoc Networks (WiMAN 2010), 2010, Zürich, Switzerland. Proceedings of ICCCN 2010/WiMAN 2010.
12. BARRETO, P. S. L. M.; Cayrel, P.; Misoczki, R.; Niebuhr, R.; 2010: “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, 2010.
13. 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), 2010, Boca Raton, USA. Proceedings of the 13th Information Security Conference (ISC 2010), 2010.
14. 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, 2009.
15. 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, 2008.
16. 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, 2008.
17. 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: Brazilian Symposium on Information and Computer Systems Security – SBSeg 2008, 2008, Gramado, Brazil. Proceedings of the 8th Brazilian Symposium on Information and Computer Systems Security – SBSeg 2008. Brazilian Computer Society (SBC), 2008.
18. 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.
19. 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, 2007.
20. 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, 2007. p. 11-16.
21. Gazzoni Filho, D. L.; BARRETO, P. S. L. M.; Rijmen, V.: "The MAELSTROM-0 Hash Function." In: Brazilian Symposium on Information and Computer Systems Security – SBSeg 2006, Santos, Brazil. Proceedings of the 6th Brazilian Symposium on Information and Computer Systems Security – SBSeg 2006. Brazilian Computer Society (SBC), 2006.
22. 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.
23. 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, 2005, Edinburgh, UK. Lecture Notes in Computer Science. Heidelberg: Springer, 2005. v. 3659. p. 412-426.
24. 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, 2005, Chennai, India.

Lecture Notes in Computer Science. Heidelberg: Springer, 2005. v. 3788. p. 515-532.
25. McCullagh, N.; BARRETO, P. S. L. M.. A New Two-Party Identity-Based Authenticated Key Agreement. In: Topics in Cryptology – CT-RSA 2005, 2005, San Francisco, USA. Lecture Notes in Computer Science. Heidelberg: Springer, 2005. v. 3376. p. 262-274.
26. BARRETO, P. S. L. M.; Naehrig, M.. Pairing-Friendly Elliptic Curves of Prime Order. In: Selected Areas in Cryptography – SAC 2005, 2005, Kingston, Canada. Lecture Notes in Computer Science. Heidelberg: Springer, 2005. v. 3897. p. 319-331.
27. BARRETO, P. S. L. M.; Scott, M.. Compressed Pairings. In: Advances in Cryptology – Crypto 2004, 2004, Santa Barbara (USA). Lecture Notes in Computer Science. Heidelberg: Springer, 2004. v. 3152. p. 140-156.
28. BARRETO, P. S. L. M.; Lynn, B.; Scott, M.. On the Selection of Pairing-Friendly Groups. In: Selected Areas in Cryptography – SAC 2003, 2003, Ottawa. Lecture Notes in Computer Science. Heidelberg: Springer, 2003. v. 3006. p. 17-25.
29. Nakahara Jr, J.; BARRETO, P. S. L. M.; Preneel, B.; Vandewalle, J.; Kim, H. Y.. Square Attacks on Reduced-Round PES and IDEA Block Cipher. 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, 2002. p. 187-195.
30. Daemen, J.; Rijmen, V.; BARRETO, P. S. L. M.. Rijndael – Beyond the AES. In: Mikulášská Kryptobesídka 2002, 2002, Prague, Czech Republic. Proc. 3rd Annual Czech and Slovak Cryptology Workshop, 2002.
31. BARRETO, P. S. L. M.; Kim, H. Y.; Lynn, B.; Scott, M.. Efficient Algorithms for Pairing-Based Cryptosystems. In: Advances in Cryptology – Crypto 2002, 2002, Santa Barbara. Lecture Notes in Computer Science. Heidelberg: Springer, 2002. v. 2442. p. 354-368.
32. BARRETO, P. S. L. M.; Lynn, B.; Scott, M.. Constructing Elliptic Curves with Prescribed Embedding Degrees. In: Security in Communication Networks – SCN 2002, 2002, Amalfi, Italy. Lecture Notes in Computer Science. Heidelberg: Springer, 2002. v. 2576. p. 263-273.
33. 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, 2001.
34. 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, 2001, Yokohama, Japan. Lecture Notes in Computer Science. Heidelberg: Springer, 2001. v. 2355. p. 165-173.
35. Kim, H. Y.; BARRETO, P. S. L. M.; 2000: Fast Binary Image Resolution Increasing by k-Nearest Neighbor Learning. In: IEEE International Conference on Image Processing, 2000, Vancouver, Canada. Proceedings, v. 2. p. 327-330.
36. BARRETO, P. S. L. M.; Kim, H. Y.; Rijmen, V.; 2000: Um Modo de Operação de Funções de Hashing para Localizar Alterações em Dados Digitalmente Assinados (in Portuguese). In: Simpósio Brasileiro de Telecomunicações (SBrT), 2000. Proc. SBrT – Simpósio Brasileiro de Telecomunicações.

37. BARRETO, P. S. L. M.; Rijmen, V.; 2000: The ANUBIS Block Cipher. In: 1st Open NESSIE Workshop, 2000, Leuven (Belgium). Proceedings of the 1st Open NESSIE Workshop.
38. BARRETO, P. S. L. M.; Rijmen, V.; 2000: The KHAZAD Legacy-Level Block Cipher. In: 1st Open NESSIE Workshop, 2000, Leuven (Belgium). Proceedings of the 1st Open NESSIE Workshop.
39. BARRETO, P. S. L. M.; Rijmen, V.; 2000: The WHIRLPOOL Hashing Function. In: 1st Open NESSIE Workshop, 2000, Leuven (Belgium). Proceedings of the 1st Open NESSIE Workshop.

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 International Publishing, 2014, p. 387-439.
2. van Tilborg, H. C. A.; Jajodia, S.; BARRETO, P. S. L. M.; Rijmen, V.; 2011:. Whirlpool. In: van Tilborg, H. C. A.; Jajodia, S. (Eds.). Encyclopedia of Cryptography and Security 2nd Edition. Springer, p. 1384-1385.
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.
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.
5. Abdalla, M.; BARRETO, P. S. L. M. (Eds.). Progress in Cryptology – LATINCRYPT 2010. Berlin/Heidelberg: Springer, 2010. 322 p.
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, 2009. 305 p.
7. Margi, C. B.; Simplício Jr., M. A.; BARRETO, P. S. L. M.; Carvalho, T. C. M. B.; 2009: 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.
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.
9. BARRETO, P. S. L. M.; Rijmen, V.; 2003: Dedicated Hash-Function 7 (Whirlpool). In: ISO/IEC. (Org.). ISO/IEC 10118-3:2003: Information technology Security techniques Hash-functions Part 3: Dedicated hash-functions. Geneva: International Organization for Standardization (ISO), p. 19-22.

Other publications:

1. V. Rijmen, BARRETO, P. S. L. M., "The Khazad Block Cipher," *The Perl Journal* **7**, p. 5, 2003.
2. BARRETO, P. S. L. M., B. Libert, N. McCullagh, J.-J. Quisquater, "Efficient and secure identity-based signatures and signcryption from bilinear maps," submission to the P1363.3 working group of the IEEE Standards Association. New Jersey, USA: IEEE, 2006.
3. BARRETO, P. S. L. M., M. Naehrig, "Pairing-Friendly Elliptic Curves of Prime Order with Embedding Degree 12," submission to the P1363.3 Working Group of the IEEE Standards Association. New Jersey, USA: IEEE, 2006.
4. BARRETO, P. S. L. M., M. Naehrig, "Elliptic curve generation – BN curves,"submission to the ISO/IEC 15946-5 working draft. Geneva, Switzerland: ISO/IEC, 2007.

Projects coordinated (academic scope):

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).

Universal CNPq 2011. Funding amount: R$ 49,980.00

Universal CNPq 2007. Funding amount: R$ 20,000.00

Projects coordinated with industry:

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 2013–2015, US$ 200,000.00 per year 2014–2016.

Scopus Tecnologia S.A. project "Security framework for digital cash," timeframe 2009–2014 (ongoing, renewed yearly). Funding amount: R$ 160.000,00 per year.

Cisco Research grant 2011-050 "Alternate Public Key Cryptosystems," 2011. Funding amount: US$ 100,000.00

Participation as consultant in other projects with industry:

Ericsson Research: Personalized mobile health solutions – security aspects (2012-2013)

National Instruments: Security Framework for LabVIEW™ (2011)

Scopus Tecnologia S/A: Lightweight PKI for Mobile Platforms (2009-2012)

Unibanco S/A: IT Security Concepts for Financial Applications (2006)

Ericsson Research: Lightweight Ciphers for Wireless Sensor Networks (2007-2010)

MBA course, several companies: Fundamentals of Information Security (2002-2008)