Curriculum Vitae

Bernardo Machado David

SUMMARY AND RESEARCH INTERESTS

I am an Associate Professor at the IT University of Copenhagen, where I conduct teaching and research on cryptographic protocols. From 2017 to 2018 I was an Assistant Professor at the Tokyo Institute of Technology. I hold a Ph.D. in Computer Science from Aarhus University obtained in 2017 under the supervision of Ivan Damgård and Jesper Buus Nielsen. I was a long-term visitor at the Cryptography Group of Bar Ilan University in Israel and the NTT Secure Platform Laboratories in Japan. My research focuses on theoretical and practical aspects of secure multiparty computation and blockchain systems, as well as the interplay between these topics. I aim at both understanding the fundamental asymptotic limits of cryptographic protocols and at constructing efficient scalable privacy preserving applications (e.g. on blockchains). My work has been supported by grants from the Japanese Society for the Promotion of Science, IOHK, Concordium Foundation, Protocol Labs and Independent Research Fund Denmark, among others. I also consult on industry projects, having advised the Cardano project and currently serving as Scientific Advisor to the blockchain company Concordium, among other projects related to cryptography.

CONTACT DETAILS

EMAIL: bernardo@bmdavid.com **TELEPHONE:** +4529883541

ADDRESS: Rued Langgaards Vej 7, 2300, Copenhagen, Denmark.
Office: 4C02

Homepage: http://www.bmdavid.com

EDUCATION

Ph.D. in Computer Science – Aarhus University, Denmark – 2017
Supervisor: Ivan Damgård, Co-Supervisor: Jesper Buus Nielsen
Thesis Title: A Framework For Efficient Homomorphic Universally Composable Commitments

M.Sc. in Computer Science – Aarhus University, Denmark – 2015
Supervisor: Ivan Damgård, Co-Supervisor: Jesper Buus Nielsen
Thesis Title: Secure Computation and Cryptographic Protocols

B.E. in Network Engineering – University of Brasilia, Brazil – 2013
Supervisor: Anderson Nascimento
Thesis Title: A Unifying Framework For Universally Composable Oblivious Transfer From Lossy Trapdoor Encryption That Yields Coding Based Protocols

EMPLOYMENT

2019-Present – IT University of Copenhagen, Denmark
Position: Associate Professor (Lektor)
Job Description: I am part of the Department of Computer Science, conducting teaching and research activities related to cryptography and security. I am also a member of the Center for Information Security Research (CIST). Moreover, I collaborate with industry partners on applying research results in cryptographic protocols to industry projects on blockchains and cryptocurrencies.

2019-Present – Concordium Research, Denmark
Position: Scientific Advisor
Job Description: I design novel scalable blockchain protocols with privacy and accountability guarantees as well as aid the engineering team in their implementation.

2017-2019 – Tokyo Institute of Technology, Japan
Position: Specially Appointed Assistant Professor
Job Description: I was part of the industry funded Input Output Cryptocurrency Collaborative Research Chair in the Department of Mathematical and Computing Sciences, conducting teaching and research activities. As part of my teaching activities, I designed and taught the first course on cryptographic protocols and blockchain technologies in the Tokyo Institute of Technology. As part of my research activities, I have worked on protocols for secure multiparty computation as well as blockchain based applications, yielding publications in top international conferences. My research was also supported by a JSPS Grant-in-Aid for Early Career Scientists.

2016-2019 – IOHK Research, Remote
Position: Research Fellow (Part-time)
Job Description: I was a part-time research fellow developing new technologies for cryptocurrencies and smart contracts. I am responsible for designing new provably secure cryptographic protocols and working with the engineering team on developing production grade implementations. I have been involved in the design and assisted in the implementation of Ouroboros, the first provably secure Proof-of-Stake based blockchain protocol, SCRAPE, a scalable publicly verifiable source of randomness and Royale, a framework for multiparty card games with financial rewards and penalties.

2013-2017 - Department of Computer Science, Aarhus University, Denmark
Position: Ph.D. Fellow
Job Description: I did research on theoretical and practical aspects of secure multiparty computation under the supervision of Ivan Damgård. In 2016, I have also spent 6 months as a visiting Ph.D. student at the Cryptography Group of Bar Ilan University. My research resulted in the most asymptotically and concretely efficient homomorphic universally composable commitment schemes at the time. Moreover, I was a teaching assistant for courses of the Department of Computer Science.

2012-2013 – IPe Network Engineering, Brazil.
Position: Partner and R&D Coordinator
Job Description: As one of the 4 partners, I coordinated research & development of new products. At IPe, I was directly involved in the conception and development of PLEASE, a user authentication system, and Vidya, a web application firewall. Moreover, I worked as a support engineer for networking, storage and Unix infrastructures.

2011-2012 – Secure Platform Laboratories, NTT Corporation, Japan
Position: Research Intern
Job Description: I worked for 6 months as an intern under the supervision of Tatsuaki Okamoto and Masayuki Abe. During this period I did research on functional encryption and structure preserving cryptography. My research resulted in the first structure preserving schemes with tight security based on standard assumptions.

Research Grants

Title: Efficient Provably Secure Blockchain Protocols and Applications
Program: JSPS Grants-in-Aid for Early Career Scientists
Role: Principal Investigator

Project Duration: 2018-2019
Amount: 4290000 JPY (about 250.000,00 DKK)
Project Description: This project yielded the first Proof-of-Stake blockchain protocol secure against adaptive adversaries in semi-synchronous networks and the first protocol for general card games with financial punishments, which is also universally composable.

Title: S^2LEGDES: Secret Single Leader Election on the Edge of Speed
Program: Research Gift from Protocol Labs
Role: Principal Investigator.
Project Duration: 2019-2020.
Amount: 60.000,00 USD (about 400.000,00 DKK with no overhead)
Project Description: This project improved committee and leader election mechanisms for blockchain consensus protocols. It involved a research assistant under my supervision.

Title: Scalable Proof-of-Stake Blockchain Consensus Protocols
Program: Research Gift from Concordium Foundation
Role: Principal Investigator
Project Duration: 2019-2022
Amount: 1.660.000,00 DKK (no overhead)
Project Description: The goal of this project is to design efficient and highly scalable Proof-of-Stake based blockchain consensus protocols with novel sharding and sidechain techniques. The project involves a PhD student under my supervision.

Title: Transaction Anonymity and Accountability in Cryptocurrencies
Program: DFF | FNU – Research Project 1
Role: Principal Investigator
Project Duration: 2019-2023
Amount: 2.879.654,00 DKK
Project Description: The goal of this project is to design schemes for anonymous cryptocurrency transactions with accountability features compatible with financial regulations. The project involves a PhD student under my supervision.

Title: PUMA: Publicly Verifiable Multiparty Computation and Applications
Program: DFF | Digital Technologies (Thematic Research 2019)
Role: Principal Investigator.
Project Duration: 2020-2023.
Amount: 2.868.716,00 DKK
Project Description: This project will investigate fundamental limits and efficient constructions of Multiparty Computation (MPC) protocols with public verifiability and other special properties such as cheater identification. The project also involves a Postdoc.

Title: Private Smart Contract på blockchain
Program: InfinITs miniprojektpulje
Role: Co-Principal Investigator.
Project Duration: 2020-2020.
Amount: 180.000,00 DKK
Project Description: This project investigated the practical applicability of techniques from my paper “Insured MPC: Efficient Secure Multiparty Computation with Punishable Abort” towards fair exchanges through a prototype implementation and benchmarks.

Title: Foundations of Privacy Preserving and Accountable Decentralized Protocols
Program: DFF Sapere Aude
Role: Principal Investigator.
Project Duration: 2021-2025.
Amount: 6.191.821,00 DKK

Project Description: This project will investigate privacy preserving and accountable protocols combining MPC and blockchain techniques. The project involves two Postdocs and a PhD student under my supervision

Title: P2DrEAMM: Privacy Preserving Decentralized Exchange Automatic Market Maker
Program: CPH Fintech (with co-funding from Monaco Foundry)
Role: co-Principal Investigator (with Carsten Baum, AU, and Tore Frederiksen, ALX).
Project Duration: 2022-2022
Amount: 300.000,00 DKK
Project Description: This project will extend my "Insured MPC" results to obtain MPC that distributes a secret amount of deposited funds among the parties according to the computation output, aiming at creating privacy preserving automated market makers.

Title: Accountable Privacy Preserving Computation via Blockchain
Program: DIREC Explorer
Role: co-Principal Investigator (with Sophia Yakoubov, AU, and Tore Frederiksen, ALX)
Project Duration: 2022-2023
Amount: 337.560,00 DKK
Project Description: This project will explore practical implementations of accountable privacy preserving computation using a blockchain ledger for coordination and verifiability.

Title: Time-based Cryptographic Primitives based on Relativistic Delay with Reduced Trust on Satellites
Program: Protocol Labs
Role: co-Principal Investigator (with Carsten Baum, AU).
Project Duration: 2022-2022
Amount: 60.000,00 USD (about 400.000,00 DKK).
Project Description: This project will investigate efficient constructions of verifiable delay functions and time lock puzzles using physical limits (minimum communication delay) instead of sequential hardness of computational problems.

Title: Privacy Preserving Solutions for Network Security (P2SNS)
Program: Global Innovation Network Program (GINP) – Danish Agency for Higher Education and Science
Role: Head of Consortium and co-Principal Investigator (with Diego Aranha from Aarhus University, Rafael Dowsley from Monash University, João Gondim from University of Brasilia and Anderson Nascimento, University of Washington).
Project Duration: 2023-2024
Amount: 691.200,00 DKK
Project Description: This project will investigate efficient privacy preserving machine learning protocols for anomalous network traffic detection.

Professional Activities and Program Committees

Program Committee Member:

- Eurocrypt 2023, 2024.
- Asiacrypt 2018, 2021, 2023.
- ICDCS 2023.
- PKC 2018, 2022.
- PODC 2020.
- Latincrypt 2021, 2023.

- CANS 2017, 2022, 2023.
- IWSEC 2019, 2020, 2021, 2023.
- NSS 2023.
- IFIP SEC 2022
- EISA 2021
- ACISP 2021
- 8th ACM SBC 2020.
- Provsec 2017, 2018, 2019.
- BlockSEA 2018
- IEEE Security & Privacy 2017 (Student Program Committee).

Event Organization:

- Contributed Talks Committee member for the PPML workshop co-located with CRYPTO 2023.

- Co-Organizer (with Carsten Baum, DTU) of the 1st Summer School on Privacy Preserving Machine Learning in 2022, held at ITU with financial support from the IACR, the Danish Data Science Academy and the Pioneer Center for AI.

- Organizer and chair of the session on "Privacy, Regulatory Compliance and High-Assurance for Blockchain Systems and WEB3" at the Digital Tech Summit 2022 in Copenhagen, an event bringing together Danish industry and academia.

Reviewer: I frequently review for conferences organized by the International Association of Cryptological Research (Asiacrypt, Crypto, Eurocrypt, PKC, TCC), security conferences (e.g. CCS and NDSS) and journals such as IET Information Security, IEEE Transactions on Information Security and Forensics, IEEE Transactions on Secure and Dependable Computing, IEEE Transactions on Service Computing, and Journal of Cryptology.

PhD Student and Postdoc Supervision

PhD Students:

- Lorenzo Gentile – Graduated in April 2023.
- James Hsin-yu Chiang (Co-Supervised with Alberto Lluch, DTU Compute) – Graduated in August 2023.
- Anders Konring – Expected to Graduate in November 2023.

Postdocs:

- Felix Engelman – January 2022 to December 2022.
- Ravi Kishore – September 2020 to July 2023.
- Esra Yeniaras – June 2023 to Present.

Teaching

Fall 2020, Fall 2021, Fall 2022, Fall 2023 – **IT University of Copenhagen – Professor – Course: Security 1**

Spring 2020, Spring 2021, Spring 2022, Spring 2023 – **IT University of Copenhagen – Professor – Course: Cryptographic Computation and Blockchain**

Fall 2019 and Fall 2020, Fall 2021 – **IT University of Copenhagen – Co-Professor – Course: Advanced Security**

Spring 2018 – **Tokyo Institute of Technology – Professor – Course: Cryptographic protocols and Blockchain Technologies**
Spring 2015 and Fall 2016 – **Aarhus University – Teaching Assistant – Course: Databases**

Spring 2014 – **Aarhus University – Teaching Assistant – Course: Distributed systems**

Fall 2013 and Fall 2014 – **Aarhus University – Teaching Assistant – Course: Advanced Physical Computing**

Spring 2013 – **Aarhus University – Teaching Assistant – Course: Introduction to Security**

Second Semester 2012 – **Brazilian Army – Instructor – Course: Introduction to Cryptography and Network Security**

Second Semester 2012 – **University of Brasilia – Teaching Assistant – Courses: Network Protocols and Architecture**

Second Semester 2010 – **University of Brasilia – Teaching Assistant – Courses: Unix Systems Forensics, MS Windows Systems Forensics.**

First Semester 2010 – **University of Brasilia – Teaching Assistant – Courses: Operating Systems 1 and Network Engineering 1**

Selected Invited Talks

- Alice in Randomland: PVSS, TLPs, VRFs, a glance thru' the looking glass of acronyms and random beacons. Randomness Summit 2023.
- MPC on Blockchains: Privacy Preserving Smart Contracts for Fun and Profit. Digital Tech Summit 2021.
- ALBATROSS: publicly AttestabLe BATched Randomness based On Secret Sharing. Monash University Blockchain Technology Center Seminar, 2020.
- TARDIS+CRAFT: UC VDFs and timelock puzzles, and their applications to fair randomness and MPC. Protocol Labs Seminar, 2020.
- Public Verifiable MPC and Applications. Joint Workshop of NTT Labs (Japan) and NTT Research (USA), 2019.
- Efficient MPC meets Blockchains. Workshop on Blockchain Technology and Theory (Co-located with PODC 2018).
- PoS Blockchain Protocols. Binary District Amsterdam 2018.
- Bitcoin, Blockchains and Applications. Infosecurity Denmark 2017.
- A Provably Secure Proof-of-Stake Blockchain Protocol. Worskhop on Cryptographic

Technologies for Securing Network Storage and Their Mathematical Modeling, Institute of Mathematics for Industry (IMI), Kyushu University, 2017.

- Recent Results on Efficient UC Commitments. Greater Tel Aviv Area Cryptography Seminar, Bar Ilan University, 2016.

- Rate-1, Linear Time and Additively Homomorphic UC Commitments. Chuo University Cryptography Seminar, 2016.

- Universally Composable Oblivious Transfer From Lossy Encryption And The McEliece Assumptions. Aarhus University Theory Seminar, 2012.

- Universally Composable Oblivious Transfer From The McEliece Assumptions. Chuo University Cryptography Seminar, 2011

PUBLICATIONS

Refereed Conference Publications (authors are in alphabetical order):

1. James Hsin-yu Chiang, Bernardo David, Ittay Eyal, Tiantian Gong. FairPoS: Input Fairness in Proof-of-Stake with Adaptive Security. AFT 2023.

2. James Hsin-yu Chiang, Bernardo David, Mariana Gama, Christian Janos Lebeda. Correlated-Output-Differential-Privacy and Applications to Dark Pools. AFT 2023.

3. Carsten Baum, James Hsin-yu Chiang, Bernardo David, Tore Kasper Frederiksen. SoK: Privacy-Enhancing Technologies in Finance. AFT 2023.

4. Bernardo David, Yuval Ishai, Anders Konring, Eyal Kushilevitz, Varun Narayanan: Perfect MPC over Layered Graphs. CRYPTO 2023.

5. Joakim Brorsson, Bernardo David, Lorenzo Gentile, Elena Pagnin, Paul Stankovski Wagner. PAPR: Publicly Auditable Privacy Revocation for Anonymous Credentials. CT-RSA 2023.

6. Ignacio Cascudo, Bernardo David, Omer Shlomovits, Denis Varlakov. Mt. Random: Multi-tiered Randomness Beacons. ACNS 2023.

7. Carsten Baum, Bernardo David, Rafael Dowsley, Ravi Kishore, Jesper Buus Nielsen, Sabine Oechsner. CRAFT: Composable Randomness Beacons and Output-Independent Abort MPC From Time. PKC 2023.

8. Carsten Baum, James Hsin-yu Chiang, Bernardo David, Tore Kasper Frederiksen: Eagle: Efficient Privacy Preserving Smart Contracts. Financial Cryptography 2023.

9. Steven Golob, Sikha Pentyala, Rafael Dowsley, Bernardo David, Mario Larangeira, Martine De Cock, Anderson Nascimento. A Decentralized Information Marketplace Preserving Input and Output Privacy. ACM 2nd Data Economy Workshop Co-Located with ACM SIGMOD 2023.

10. Ignacio Cascudo, Bernardo David, Lydia Garms, Anders Konring. YOLO YOSO: Fast and Simple Encryption and Secret Sharing in the YOSO Model. ASIACRYPT 2022.

11. Matteo Campanelli, Bernardo David, Hamidreza Khoshakhlagh, Anders Konring, Jesper Buus Nielsen. Encryption to the Future: A Paradigm for Sending Secret Messages to Future (Anonymous) Committees. ASIACRYPT 2022.

12. Carsten Baum, Bernardo David, Rafael Dowsley. A Framework for Universally Composable Publicly Verifiable Cryptographic Protocols. ProvSec 2022.

13. Bernardo David, Bernardo Magri, Christian Matt, Jesper Buus Nielsen, Daniel Tschudi. GearBox. An Efficient UC Sharded Ledger Leveraging the Safety-Liveness Dichotomy. CCS 2022.

14. Carsten Baum, James Hsin-yu Chiang, Bernardo David, Tore Kasper Frederiksen, Lorenzo Gentile. SoK: Mitigation of Front-running in Decentralized Finance. 2nd Workshop on Decentralized Finance, Financial Cryptography 2022.

15. Bernardo David, Lorenzo Gentile, Mohsen Pourpouneh. FAST: Fair Auctions via Secret Transactions. ACNS 2022.

16. Carsten Baum, Bernardo David, Tore Frederiksen. P2DEX: Privacy-Preserving Decentralized Cryptocurrency Exchange. ACNS 2021.

17. Carsten Baum, Bernardo David, Rafael Dowsley, Jesper Buus Nielsen, Sabine Oechsner. TARDIS: Foundations of Time-Lock Puzzles in UC. Eurocrypt 2021.

18. Bernardo David, Rafael Dowlsey. Efficient Composable Oblivious Transfer from CDH in the Global Random Oracle Model. CANS 2020.

19. Ignacio Cascudo, Bernardo David. ALBATROSS: publicly AttestabLe BATched Randomness based On Secret Sharing. ASIACRYPT 2020.

20. Carsten Baum, Bernardo David, Rafael Dowsley. Insured MPC: Efficient Secure Multiparty Computation with Punishable Abort. Financial Cryptography 2020.

21. Ignacio Cascudo, Ivan Damgård, Bernardo David, Rafael Dowsley, Nico Döttling, Irene Giacomelli. Efficient UC Commitment Extension with Homomorphism for Free (and Applications). ASIACRYPT 2019.

22. Bernardo David, Rafael Dowsley, Mario Larangeira. Royale: A Framework for Universally Composable Card Game with Financial Rewards and Penalties Enforcement. Financial Cryptography 2019.

23. Bernardo David, Rafael Dowsley, Mario Larangeira. MARS: Monetized Ad-hoc Routing System (A Position Paper). ACM MobiSys – CryBlock 2018.

24. Bernardo David, Peter Gazi, Aggelos Kiayias, Alexander Russell. Ouroboros Praos: An Adaptively-Secure, Semi-synchronous Proof-of-Stake Blockchain. EUROCRYPT 2018.

25. Bernardo David, Rafael Dowsley, Mario Larangeira. Kaleidoscope: An Efficient Poker Protocol with Payment Distribution and Penalty Enforcement. Financial Cryptography 2018.

26. Bernardo David, Rafael Dowsley, Mario Larangeira. 21 - Bringing Down the Complexity. Fast Composable Protocols for Card Games Without Secret State.

ACISP 2018.

27. Aggelos Kiayias; Alexander Russel; Bernardo David; Roman Oliynykov: Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. CRYPTO 2017

28. Ignacio Cascudo; Bernardo David: SCRAPE: Scalable Randomness Attested by Public Entities. ACNS 2017

29. Ignacio Cascudo; Ivan Damgård; Bernardo David; Nico Döttling; Jesper Buus Nielsen: Rate-1, Linear Time and Additively Homomorphic UC Commitments. CRYPTO 2016

30. Bernardo David; Rafael Dowsley; Raj Katti; and Anderson C. A. Nascimento: Efficient Unconditionally Secure Comparison and Privacy Preserving Machine Learning Classification Protocols. Provsec 2015.

31. Bernardo David; Ryo Nishimaki; Samuel Ranellucci; Alain Tapp: Generalizing Efficient Multiparty Computation. ICITS 2015.

32. Ignacio Cascudo; Ivan Damgård; Bernardo David; Irene Giacomelli; Jesper Buus Nielsen; Roberto Trifiletti: Additively Homomorphic UC commitments with Optimal Amortized Overhead. PKC 2015.

33. Ivan Damgård; Bernardo David; Irene Giacomelli; Jesper Buus Nielsen: Compact VSS and Efficient Homomorphic UC Commitments. Asiacrypt 2014.

34. Bernardo David; Rafael Dowsley; Anderson C. A. Nascimento: Universally Composable Oblivious Transfer based on a variant of LPN. CANS 2014.

35. Masayuki Abe; Bernardo David; Markulf Kohlweiss; Ryo Nishimaki; Miyako Ohkubo: Tagged One-Time Signatures: Tight Security and Optimal Tag Size. PKC 2013.

36. Masayuki Abe; Melissa Chase; Bernardo David; Markulf Kohlweiss; Miyako Okhubo; Ryo Nishimaki. Constant-Size Structure Preserving Signatures: Generic Constructions and Simple Assumptions. Asiacrypt 2012.

37. Bernardo David, Anderson C. A. Nascimento, Rafael T. M. Quelho, Rafael Timóteo de Sousa Júnior. A framework for secure single sign-on. Workshop de Gestão de Identidades Digitais, SBSEG 2012.

38. Bernardo David; João Paulo C. L. Costa, Dino Amaral, Rafael Timóteo de Sousa Júnior, Edson P. FREITAS, A. M. R. SERRANO. Improved Blind Automatic Malicious Activity Detection in Honeypot Data. ICoFCS 2012.

39. Adriana Pinto; Bernardo David; Anderson C. A. Nascimento; Jeroen Van de Graaf. Universally Composable Committed Oblivious Transfer with a Trusted Initializer. SBSEG 2012.

40. Bernardo David, Anderson C. A. Nascimento; Jörn Müller-Quade. Universally Composable Oblivious Transfer From Lossy Encryption And The McEliece Assumptions. Proceedings of the 6th International Conference on Information Theoretic Security – ICITS 2012.

41. Bernardo David, Anderson C. A. Nascimento. Efficient fully simulatable oblivious transfer from the McEliece assumptions. IEEE Information Theory Workshop (ITW), 2011, p. 638-642.

42. Rafael T. M. Quelho, Bernardo David, Vinicius M. Alves. Universally Composable Private Proximity Testing. ProvSec - Proceedings of the 5th international conference on Provable security, 2011, p. 222-239.

43. Bernardo David, Rafael T. M. Quelho, Anderson C. A. Nascimento . Obtaining Efficient Fully Simulatable Oblivious Transfer from General Assumptions. Anais do XI Simposio Brasileiro de Segurança da Informação e de Sistemas Computacionais, 2011, p. 108-121.

44. Marcelo D. Holtz, Bernardo David, Rafael T. S. Júnior. An architecture for distributed Network Intrusion Detection based on the Map-Reduce Framework. Proceedings of The International Workshop on Telecommunications - IWT 2011, p. 106-110.

45. Bernardo David, João Paulo C. L. da Costa, Anderson C. A. Nascimento, Marcelo D. Holtz, Dino Amaral, Rafael T. S. Júnior. Blind Automatic Malicious Activity Detection in Honeypot Data. Proceeding of the Sixth International Conference on Forensic Computer Science ICoFCS 2011, 2011, p. 142-152.

46. Bernardo David, Anderson C. A. Nascimento, Rodrigo Nogueira . Oblivious Transfer Based on the McEliece Assumptions with Unconditional Security for the Sender. Anais do Simpósio Brasileiro de Segurança da Informação 2010, 2010.

47. Bernardo David, Rafael T. S. Júnior. A Bayesian Trust Model for the MAC Layer in IEEE 802.15.4 Networks. Proceedings of The 9th Information and Telecommunication Technologies Symposium, 2010, p. 105-111.

Journal Publications:

1. Bernardo David, Rafael Dowsley, Jeroen van de Graaf, Davidson Marques, Anderson C. A. Nascimento, Adriana C. B. Pinto. Unconditionally Secure, Universally Composable Privacy Preserving Linear Algebra. IEEE Trans. Information Forensics and Security 11(1): 59-73 (2016).

2. Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, Miyako Ohkubo. Constant-Size Structure-Preserving Signatures: Generic Constructions and Simple Assumptions. J. Cryptology 29(4): 833-878 (2016).

3. Bernardo David, Anderson C. A. Nascimento. Fully Simulatable Oblivious Transfer Based on The McEliece Assumptions. IEICE Transactions 95-A(11): 2059-2066 (2012).

4. Bernardo David, João Paulo C. L. da Costa, Anderson C. A. Nascimento, Marcelo D. Holtz, Dino Amaral, Rafael T. S. Júnior. A Parallel Approach to PCA Based Malicious Activity Detection in Distributed Honeypot Data. The International Journal of Forensic Computer Science (Printed), v. 6, p. 8-27, 2011.

5. Marcelo D. Holtz, Bernardo David, Rafael T. S. Júnior. Building Scalable Distributed Intrusion Detection Systems Based on the MapReduce Framework. Telecomunicações (Santa Rita do Sapucaí), v. 13, p. 22-31, 2011.

6. Laerte Peotta, Marcelo D. Holtz, Bernardo David, Flávio G. Deus, Rafael T. S. Júnior . A Formal Classification of Internet Banking Attacks and Vulnerabilities. International Journal of Computer Science and Information Technology, v. 3, p. 186-197, 2011.

7. Bernardo David, Beatriz Santana, Laerte Peotta, Marcelo D. Holtz, Rafael T. S. Júnior. A Context-Dependent Trust Model for the MAC Layer in LR-WPANs. International Journal on Computer Science and Engineering, v. 2, p. 3007-3016, 2010.