**Curriculum Vitae**

**Bernardo Machado David**

## CAREER SUMMARY

From June 2017, I will be an Assistant Professor at the Computer Science Department of the Tokyo Institute of Technology. My main research interests are in theoretical and practical aspects of secure multiparty computation and cryptographic protocols in general. I hold a Ph.D. in Computer Science from Aarhus University obtained in 2017 under the supervision of Ivan Damgård. I was a visiting PhD Student at the Cryptography Group of Bar Ilan University working with Yehuda Lindell for the first half of 2016. During the last year of my Ph.D., I have also done consultancy on cryptographic protocols, collaborating with industry partners on the design and implementation of provably secure cryptocurrency and smart contract solutions. Before starting my Ph.D. I have worked as an undergraduate student at University of Brasilia under the supervision of Anderson C. A. Nascimento. I spent six months from 2011 to 2012 as a research intern at the NTT Secure Platform Laboratories, Tokyo, Japan under the supervision of Tatsuaki Okamoto and Masayuki Abe. I have also done research on structure preserving signatures, intrusion detection systems, wireless sensor network security, practical user authentication and online banking. Besides academic research, I have experience in information technology and security, having worked on consultancy projects for the Brazilian government and private institutions

## CONTACT DETAILS

**EMAIL:** bernardo@bmdavid.com **TELEPHONE:** +45 29883541

**ADDRESS:** Department of Computer Science, Aabogade 34, 8200 Aarhus, Denmark. Office: Nygaard 284

**Homepage:** http://www.bmdavid.com

## EDUCATION

**Aarhus University – Ph.D. in Computer Science – 2017**
**Supervisor: Ivan Damgård**

**Aarhus University – M.Sc. in Computer Science – 2015**
**Supervisor: Ivan Damgård**

**University of Brasilia – B.E. in Network Engineering – 2013**
**Supervisor: Anderson Nascimento**

## EMPLOYMENT

**2016-Present – IOHK Research, Remote**
**Position:** Research Fellow (Part-time)
**Job Description:** I am 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, and SCRAPE, a scalable publicly verifiable source of randomness.

**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. Besides doing research, I was a teaching assistant for the following courses of the Department of Computer Science of Aarhus University: Introduction to Security, Distributed Systems, Advanced Physical Computing and Databases.

**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.

**2011-2011 – University of Brasilia – SOF Joint Project: Data Modeling and Multidimensional Extraction of Federal Budget data for the Brazilian Department of Federal Budget (Secretaria do Orçamento Federal – SOF)**
**Position:** Network Engineering Intern
**Job Description:** I was responsible for assessing current infrastructure and implementing the new information security policy of the Department of Federal Budget, including adapting the data center infrastructure.

**2010-2010 – University of Brasilia – Brazilian Department of Federal Police Joint Project: Digital Forensics Professional Masters Program**
**Position:** Teaching Assistant
**Job Description:** Creation of the distance learning material used in the Digital Forensics Masters Program offered by the University of Brasília to the Brazillian Department of Federal Police. Teaching Assistant in the following courses: Operating Systems 1, Network Egineering 1, Network Engineering 2, Unix Systems Forensics, MS Windows Systems Forensics.

**2010-2010 – University of Brasilia -Dell Computers of Brazil Joint Project: LATITUDE**
**Position:** Network Engineering Intern
**Job Description:** Coordinated the deployment and administration of the Business Intelligence Lab datacenter, being responsible for the installation and administration of network infrastructure, storage systems and production servers.

**2010-2010 – University of Brasilia-SPU Joint Project: Integration of IT Services, IT Management and IT Systems to the Business Intelligence system of the Brazilian Department of Federal Realty Estate (Secretaria de Patrimônio da União).**
**Position:** Network Engineering Intern
**Job Description:** Analysis of the current IT infrastructure and business processes of the Brazillian Department of Federal Realty State. Proposition of new IT business processes and guidelines for achieving adherence to IT management Best practices

based on ITIL v2.

**2009-2010 – Network Engineering Laboratory – Department of Electrical Engineering / University of Brasilia**
**Position:** Network Engineering Intern
**Job Description:** Linux/Unix systems administration (Red Hat, CentOS, FreeBSD) and Windows Server administration (Exchange Server, Active Directory, IIS). Cisco network administration. Management and administration of information security policies and mechanisms.

**2008-2010** – **Engnet Consultoria e Implementacão (Junior Telecommunications Engineering Student's Company)**
**Position:** Junior Consultant
**Job Description:**– Deployment of a virtualized Firewall environment and network restructuring for NTI-UnB. Organization and teaching of a Linux Systems Administration course. Restructuring of the Electrical Engineering Department of the University of Brasilia servers.

**2009-2009 – Scientific High Performance Computing Laboratory – Physics Department/University of Brasilia**
**Position:** Network Engineering Intern
**Job Description:** Linux/Unix systems administration (Mandriva, FreeBSD, OpenBSD, Solaris, Tru64 Unix), network administration, user support, deployment of an LDAP based centralized authentication system, deployment of an automatic operating system images management and installation system for the HPC compute environment.

## PUBLICATIONS

**Refereed Conference Publications:**

1. Aggelos Kiayias; Alexander Russal; Bernardo David; Roman Oliynykov: Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. In: Crypto 2017

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

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

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

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

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

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

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

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

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

11. Bernardo David ; Anderson C. A. Nascimento ; QUELHO, R. T. M. ; Rafael Timóteo de Sousa Júnior . A framework for secure single sign-on. In: Workshop de Gestão de Identidades Digitais, SBSEG 2012.

12. Bernardo David; da Costa, J. P. C. L. ; Amaral, D. ; Rafael Timóteo de Sousa Júnior ; FREITAS, E. P. ; SERRANO, A. M. R. . Improved Blind Automatic Malicious Activity Detection in Honeypot Data. In: ICoFCS 2012.

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

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

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

16. Quelho, R. T. M. ; Bernardo David ; Alves, V. M. . Universally Composable Private Proximity Testing. In: ProvSec - Proceedings of the 5th international conference on Provable security, 2011, p. 222-239.

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

18. Holtz, M. D. ; Bernardo David ; Sousa Jr., R. T. . An architecture for distributed Network Intrusion Detection based on the Map-Reduce Framework. In: Proceedings of The Internation Workshop on Telecommunications - IWT 2011, p. 106-110.

19. Bernardo David ; da Costa, J. P. C. L. ; Anderson C. A. Nascimento ; Holtz, M. D. ; Amaral, D. ; Sousa Jr., R. T. . Blind Automatic Malicious Activity Detection in Honeypot Data. In: Proceeding of the Sixth International Conference on Forensic Computer Science ICoFCS 2011, 2011, p. 142-152.

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

21. Bernardo David ; Sousa Jr., R. T. . A Bayesian Trust Model for the MAC Layer in IEEE 802.15.4 Networks. In: 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. In: 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. In: J. Cryptology 29(4): 833-878 (2016).

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

4. Bernardo David; da Costa, J. P. C. L. ; Anderson C. A. Nascimento ; Holtz, Marcelo D. ; Amaral, D. ; Sousa Jr., R. T. . A Parallel Approach to PCA Based Malicious Activity Detection in Distributed Honeypot Data. The International Journal of Forensic Computer Science (Impresso), v. 6, p. 8-27, 2011.

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

6. Peotta, Laerte ; Holtz, Marcelo D. ; Bernardo David ; Deus, Flavio G. ; Timoteo de Sousa, Rafael . 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 ; Santana, B. ; Peotta, L. ; Holtz, M. D. ; Sousa Jr., R. T. . 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.