Fernando Krell

Curriculum Vitæ

Education

2010-2015	**Ph.D. (Computer Science)**, *Columbia University*, New York, USA. Adviser: Prof. Tal Malkin. Area of research: Cryptography.
2014	**M.Phil. (Computer Science)**, *Columbia University*, New York, USA.
2013	**M.Sc. (Computer Science)**, *Columbia University*, New York, USA.
2003-2009	**Engineering Degree (Computer Science)**, *Universidad de Chile*, Santiago, Chile.
2006	**Bachelor Degree (Engineering Sciences)**, *Universidad de Chile*, Santiago, Chile.

Work Experience

Jan. 2022– Dec. Present	**Vice President of Engineering**, *Translucense Research Inc.*. Manage research & development department, engineering projects and hiring. Collaborate with Product Department to define goals and scope of engineering projects, and make sure requirements are met.
Nov. 2020–Dec. 2021	**Head of Cryptography Engineering**, *Translucense Research Inc.*. Manage Translucence's Cryptography Engineering team for the research and development of zero-knowledge cryptographic technology.
Jan. 2019–Oct. 2020	**Lead Cryptography Engineer**, *Eian Labs*. Led the cryptography team in the design and development of Findora's cryptographic library.
Jan. 2016–Dec. 2018	**Research & Development Engineer**, *Dreamlab Technologies AG*. Research and development of cryptographic solutions to diminish netweork communication pattern leakage.
June–Aug. 2014	**Summer Research Intern**, *SRI International*, with Dr. Gabriela Ciocarlie, Dr. Ashish Gehani and Dr. Mariana Raykova. Low leakage sublinear private search.
June–Aug. 2012	**Summer Research Intern**, *Alcatel-Lucent Bell Labs*, with Dr. Vladimir Kolesnikiov. Blind Seer: A Scalable Private DBMS.
Dec. 2007–Jan. 2008	**Summer Intern**, *Synopsys R&D Chile*. Implementation of Optimization Library in C++.
Dec. 2006–Jan. 2007	**Summer Intern**, *Adexus SA*. Developer of cluster architecture using Java CAPS.
Dec. 2006–Jan. 2007	**Summer Intern**, *Servicio de Registro Civil Chile*.

Teaching Experience

2016–2018	**Lecturer**, *Pontificia Universidad Católica de Chile*, Santiago, Chile. ○ Fall 2018: IIC3253 – Cryptography and Computational Security (in Spanish). ○ Fall 2017: IIC3253 – Cryptography and Computational Security (in Spanish). ○ Fall 2016: IIC3253 – Cryptography and Computational Security (in Spanish).
2010–2014	**Teaching Assistant**, *Columbia University*, New York. ○ Spring 2014: COMS 4995 – Cryptography and Financial Processes. Instructor: Prof. Michael Rabin. ○ Spring 2013: COMS 6261 – Advanced Cryptography: Homomorphic Encryption and Lattices. Instructors: Prof. Tal Malkin, Dr. Shai Halevi. ○ Fall 2011: COMS 4261 – Introduction to Cryptography. Instructor: Prof. Tal Malkin.
2003–2009	**Teaching Assistant**, *Universidad de Chile*, Santiago. ○ Fall 2009: CC1001 – Introduction to Computing. Instructor: Prof. Valeria Herskovic. ○ Spring 2008: CC50H – Computer Network Programming. Instructor: Prof. Nelson Baloian. ○ Fall 2008: CC41B – Operating Systems. Instructor: Prof. José Miguel Piquer. ○ Fall 2008: CC100 – Introduction to Computing. Instructor: Prof. Valeria Herskovic. ○ Spring 2007: SD20A – Design Seminar. Instructor: Prof. José Miguel Piquer. ○ Fall 2007: CC100 – Introduction to Computing. Instructor: Prof. Valeria Herskovic. ○ Fall 2007: CC30B – Computer Science Theory. Instructor: Prof. Alejandro Hevia. ○ Fall 2006: CC30A – Algorithms and Data Structures. Instructor: Prof. Patricio Poblete. ○ 2006: CC10A – Introduction to Computing. Instructor: Prof. Valeria Herskovic.

Research Projects

2014-2015 **Low-Leakage Sublinear Outsourced Private Search**, with Dr. Gabriela Ciocalie, Dr. Ashish Gehani, and Dr. Mariana Raykova.

2012-2014 **Blind Seer: A scalable private DBMS**, *Columbia University*, with Prof. Steven M. Bellovin, Dr. Seung Geol Choi, Ben Fisch, Prof. Angelos Keromytis, Dr. Vladimir Kolesnikov, Dr. Abishek Kumarasubramanian, Prof. Tal Malkin, Binh Vo, and Dr. Vasilis Pappas.

2011-2012 **Secure Computation in Sublinear Time**, *Columbia University*, with Dr. S. Dov Gordon, Prof. Jonathan Katz, Dr. Vladimir Kolesnikov, Prof. Tal Malkin, Dr. Mariana Raykova, and Dr. Yevgeniy Vahlis .

2009-2010 **Compressed Indexing of Dynamic Text Collections**, *Universidad de Chile*, with Prof. Gonzalo Navarro.

2008-2009 **Secure Distributed Backup System**, *Universidad de Chile*, with Prof. Alejandro Hevia.

Publications

Conference papers

Philippe Camacho and Fernando Krell. Asynchronous provably-secure hidden services. In *CT-RSA 2018: The Cryptographers' Track at the RSA Conference 2018, San Francisco, CA, USA, April 16 - 20*, 2018.

Fernando Krell, Gabriela Ciocarlie, Ashish Gehani, and Mariana Raykova. Low-leakage secure search for boolean expressions. In *CT-RSA 2017: The Cryptographers' Track at the RSA Conference 2017, San Francisco, CA, USA, February 14 - 17*, 2017.

Ben Fisch, Binh Vo, Fernando Krell, Abishek Kumarasubramanian, Vladimir Kolesnikov, Tal Malkin, and Steven M. Bellovin. Malicious-client security in blind seer: A scalable private dbms. In *2015 IEEE Symposium on Security and Privacy, SP 2015, San Jose, CA, USA, May 18-20, 2015*, 2015.

Vasilis Pappas, Fernando Krell, Binh Vo, Vladimir Kolesnikov, Tal Malkin, Seung Geol Choi, Wesley George, Angelos D. Keromytis, and Steve Bellovin. Blind seer: A scalable private DBMS. In *2014 IEEE Symposium on Security and Privacy, SP 2014, San Jose, CA, USA, May 18-21, 2014*, pages 359–374, 2014.

S. Dov Gordon, Jonathan Katz, Vladimir Kolesnikov, Fernando Krell, Tal Malkin, Mariana Raykova, and Yevgeniy Vahlis. Secure two-party computation in sublinear (amortized) time. In *the ACM Conference on Computer and Communications Security, CCS'12, Raleigh, NC, USA, October 16-18, 2012*, pages 513–524, 2012.

Manuscripts

Ben Fisch, Binh Vo, Fernando Krell, Abishek Kumarasubramanian, Vladimir Kolesnikov, Tal Malkin, and Steven M. Bellovin. Malicious-client security in blind seer: A scalable private dbms. Cryptology ePrint Archive, Report 2014/963, 2014. `http://eprint.iacr.org/`.

Theses

Fernando Krell Loy. *Secure Computation Towards Practical Applications*. PhD thesis, Graduate School of Arts and Sciences, Columbia University, 116th Street and Broadway, New York, NY, USA, 2015.

Fernando Krell Loy. Implementación y estudio de seguridad de un sistema de respaldo de datos distribuido. Undergraduate honors thesis, Escuela de Ingeniería y Ciencias, Universidad de Chile, Beauchef 850, Santiago, Chile, 2009.

Awards and Honors

2009 **Doctoral Scholarship**, *Becas Chile Doctorado*, CONICYT, Chile.

2008 **Outstanding Student**, *Escuela de Ingeniería y Ciencias, Universidad de Chile*, Chile.

2007 **Outstanding Student**, *Escuela de Ingeniería y Ciencias, Universidad de Chile*, Chile.

2002 **Perfect Score on "Prueba de Aptitud Académica" (Chilean Nation-wide Standardized Test) Mathematics**, Chile.

Languages

English Full professional proficiency.

Spanish Native.

Skills

Programming	Rust, C, C++, Python, JAVA
Computer Science	Advanced Cryptography, Algorithms & Data structures, Computational Complexity, LaTeX