Igors Stepanovs

E–mail	istepanovs@ethz.ch, igors.stepanovs@gmail.com
Webpage	https://sites.google.com/site/igorsstepanovs/

Conference Papers

M. Bellare and I. Stepanovs. **Security under Message-Derived Keys: Signcryption in iMessage**. In A. Canteaut and Y. Ishai, editors, *EUROCRYPT 2020, Part III*, volume 12107 of *LNCS*, pages 507–537. Springer, Heidelberg, May. 2020.

M. Drijvers, K. Edalatnejad, B. Ford, E. Kiltz, J. Loss, G. Neven, and I. Stepanovs. **On the Security of Two-Round Multi-Signatures**. In *2019 IEEE Symposium on Security and Privacy (S&P)*, pages 780-797. IEEE Computer Society Press, May 2019.

J. Jaeger and I. Stepanovs. **Optimal Channel Security Against Fine-Grained State Compromise: The Safety of Messaging**. In H. Shacham and A. Boldyreva, editors, *CRYPTO 2018, Part I*, volume 10991 of *LNCS*, pages 33-62. Springer, Cham, Aug. 2018.

M. Bellare, A. O'Neill, and I. Stepanovs. **Forward-Security under Continual Leakage**. In S. Capkun and S. Chow, editors, *CANS 2017*, volume 11261 of *LNCS*, pages 3-26. Springer, Cham, Nov. 2018.

M. Bellare, A.C. Singh, J. Jaeger, M. Nyayapati, and I. Stepanovs. **Ratcheted Encryption and Key Exchange: The Security of Messaging**. In J. Katz and H. Shacham, editors, *CRYPTO 2017, Part III*, volume 10403 of *LNCS*, pages 619–650. Springer, Cham, Aug. 2017.

M. Bellare, I. Stepanovs, and B. Waters. **New Negative Results on Differing-Inputs Obfuscation**. In M. Fischlin and J. S. Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 792–821. Springer, Heidelberg, May. 2016.

M. Bellare, I. Stepanovs, and S. Tessaro. **Contention in Cryptoland: Obfuscation, Leakage and UCE**. In E. Kushilevitz and T. Malkin, editors, *TCC 2016-A, Part II*, volume 9563 of *LNCS*, pages 542–564. Springer, Heidelberg, Jan. 2016.

M. Bellare and I. Stepanovs. **Point-Function Obfuscation: A Framework and Generic Constructions**. In E. Kushilevitz and T. Malkin, editors, *TCC 2016-A, Part II*, volume 9563 of *LNCS*, pages 565–594. Springer, Heidelberg, Jan. 2016.

M. Bellare, I. Stepanovs, and S. Tessaro. **Poly-many hardcore bits for any one-way function and a framework for differing-inputs obfuscation**. In P. Sarkar and T. Iwata, editors, *ASIACRYPT 2014, Part II*, volume 8874 of *LNCS*, pages 102–121. Springer, Heidelberg, Dec. 2014.

Employment

Feb 2020 — Sep 2021 **ETH Zürich**
Postdoctoral researcher
Working in the Applied Cryptography group, led by Prof. Kenny Paterson.

Sep 2019 — Dec 2019 **University of California, San Diego**
Mar 2019 — Jun 2019 *Teaching Assistant*
Sep 2018 — Dec 2018 CSE 105: Automata and Computability Theory (Prof. Shachar Lovett; Spring 2019)
Jan 2018 — Jun 2018 CSE 105: Automata and Computability Theory (Prof. Daniele Micciancio; Winter 2015)
Sep 2016 — Dec 2016 CSE 107: Intro to Modern Cryptography (Prof. Mihir Bellare; Winter 2018, Fall 2018)
Sep 2015 — Dec 2015 CSE 207: Modern Cryptography (Prof. Mihir Bellare; Spring 2015, Fall 2015, Fall 2016, Spring
Jan 2015 — Jun 2015 2018, Fall 2019)

Version of 15 April 2021

Jul 2019 — Dec 2019
Jan 2017 — Dec 2017
Jan 2016 — Aug 2016
Mar 2014 — Dec 2014

University of California, San Diego
Graduate Student Researcher

Supervised by: Mihir Bellare, Daniele Micciancio, Hovav Shacham.

Jun 2015 — Sep 2015

Georgetown University
Research Assistant

Supervised by Adam O'Neill.

Sep 2012 — Sep 2013

whiteCryption, Rīga, Latvia
Cryptography Researcher

Studied fully homomorphic encryption (the main focus), functional encryption, and other selected topics related to white-box cryptography. Implemented a Sage prototype of AES algorithm protected by a fully homomorphic encryption scheme.
Reviewed the product-oriented research, revolving around the ideas of secure and fast implementations of various cryptographic algorithms by using primitive operations of a virtual white-box machine.
Environment: Sage, LaTeX

Sep 2012 — May 2013
Feb 2007 — Feb 2010
(evening/weekend job)

School of Programming 'Progmeistars', Rīga, Latvia
Programming Teacher

Delivered lectures and practice lessons. Classes of high school students, in groups of 8 to 12. Curriculum highlights: programming in Pascal, Boolean logic and binary operations, DOS and FAT internals, databases (using dBASE), numerical methods, basic data structures, recursion, combinatorial algorithms.

Aug 2010 — Sep 2011

whiteCryption, Rīga, Latvia
Software Developer

Participated in the development of the 'SecureKeyBox' white-box cryptography library. Implemented various cryptography primitives using the operations of a virtual whitebox machine.
High involvement in the full development cycle. Responsible for the communication with clients concerning the functionality of the 'SecureKeyBox' library.
Environment: C++, C#, Python

Feb 2009 — Aug 2010

DnB Nord Bank, Core Banking Group, Rīga, Latvia
System Analyst / Developer

Developed a tool to parse and modify XML and XSD files. Redesigned the internal staff access control system. Maintained the payment system.
Environment: OpenEdge Advanced Business Language, Java, XML, XSD

Jul 2007 — Jan 2009
(part-time employment)

Syncrosoft, Rīga, Latvia
Software Developer

Adapted an open source parser 'Elsa' to modify C/C++ source code by changing its abstract syntax tree. Developed an automated refactoring tool for C/C++ code. Developed new features for the MCFACT software protection technology (acquired by whiteCryption in 2010).
Environment: C/C++, Python, Yaxx, Bison

Education

Sep 2013 — Dec 2019

University of California, San Diego (San Diego, USA)
Department of Computer Science and Engineering
PhD in Computer Science

Academic advisor: Prof. Mihir Bellare.

Sep 2011 — Sep 2012 **Royal Holloway, University of London** (Egham, United Kingdom)
Department of Mathematics
Master of Science in Mathematics of Cryptography and Communcations

Average grade: 81.88 out of 100 (pass with distinction). Dissertation: "A Survey of Fully Homomorphic Encryption" (supervisor: Prof. James McKee, mark: 90%).

Aug 2010 — July 2012 **University of Latvia** (Rīga, Latvia)
Faculty of Computing
Master of Science in Computer Science

Average grade: 9.475 out of 10 (diploma with distinction). Thesis: "Query Complexity of Boolean Functions with Low Polynomial Degree" (supervisor: Prof. Andris Ambainis, mark: 10 out of 10).

Sep 2006 — July 2010 **University of Latvia** (Rīga, Latvia)
Faculty of Computing
Bachelor of Science in Computer Science

Average grade: 9.337 out of 10 (diploma with distinction). Thesis: "Query Complexity of Boolean Functions with Low Polynomial Degree" (supervisor: Prof. Rūsiņš Mārtiņš Freivalds, mark: 10 out of 10)

Sep 2002 — May 2005 **School of Programming 'Progmeistars'** (Rīga, Latvia)
Special group with profound study of math and computer science, 544-hour course

Curriculum highlights: complex data structures, introduction to mathematical logic, algorithm design and analysis, generating functions, sorting and combinatorial algorithms, graph theory algorithms, flow networks, information theory and the structure of codes, text processing algorithms, the basics of cryptography and cryptanalysis, arithmetic algorithms, computational geometry algorithms, linear programming, mathematical models in economy, mathematical models in biology, introduction to numerical methods.

Programming Competitions

International Olympiad in Informatics	IOI 2006 — bronze medal IOI 2005 — silver medal
Baltic Olympiad in Informatics	BOI 2006 — bronze medal BOI 2005 — silver medal BOI 2004 — bronze medal

Technical Skills

Programming Languages	C/C++, Python & Sage, Pascal
Office automation	LaTeX

Languages

Latvian, Russian	Native languages
English	Fluent