Igors Stepanovs

E-mail: igors.stepanovs@gmail.com
Web page: https://igors.org/

3 March 2024

Education

09/2013 – 12/2019 **PhD in Computer Science**
University of California, San Diego (San Diego, USA).
Advisor: Prof. Mihir Bellare.

09/2011 – 09/2012 **MSc in Mathematics of Cryptography and Communications**
Royal Holloway, University of London (Egham, United Kingdom).
Pass with distinction (final average: 81.88/100).

08/2010 – 07/2012 **MSc and BSc in Computer Science**
09/2006 – 07/2010 University of Latvia (Rīga, Latvia).
Diplomas with distinction (weighed average grades: 9.475/10 and 9.337/10).

Employment

02/2020 – 09/2021 **Postdoctoral Researcher**
ETH Zürich (Zürich, Switzerland).
Worked in the Applied Cryptography Group led by Prof. Kenneth G. Paterson.

09/2012 – 09/2013 **Programmer**
08/2010 – 09/2011 whiteCryption (Rīga, Latvia).
Performed research and development of whitebox cryptography library `SecureKeyBox`. Wrote custom implementations of various cryptographic primitives in `C++` to leverage auxiliary instructions of an in-house source-code protection technology `MCFACT` (providing an interface to a virtual whitebox machine). Explored the feasibility of using fully homomorphic encryption (`FHE`), i.e. implemented an `FHE` scheme in `Sage`, and then implemented `AES` to use an `FHE`-encrypted secret key. In the early stages of the project, concurrently performed other roles: release engineering, communication with prospective customers.
Primarily worked with: `C++`, `Sage`, `Python`.

02/2009 – 08/2010 **System Analyst / Developer**
DnB Nord Bank (Rīga, Latvia).
Worked in the Core Banking team. Developed a tool in `Java` to parse and modify `XML` and `XSD` files.
Primarily worked with: `OpenEdge Advanced Business Language`, `Java`.

07/2007 – 01/2009 **Programmer**
Syncrosoft (Rīga, Latvia).
Built an ad-hoc `C++` refactoring tool based on `Yacc`/`Bison`. Then repurposed the open-source parser `Elsa` to (instead) refactor `C++` code by traversing its abstract syntax tree. Used it to automate the application of an in-house source-code protection technology `MCFACT` on demarcated blocks of `C++` code.
Primarily worked with: `C++`.

09/2012 – 05/2013 **Programming Teacher**
02/2007 – 02/2010 Progmeistars (Rīga, Latvia).
(part-time job) Taught programming to groups of high school students. Developed lectures and lab exercises. Covered a range of topics across different semesters, including binary arithmetic, `SQL` databases, dynamic memory allocation in `Pascal`, pointer-based data structures, recursion, and combinatorial algorithms.

Programming competitions

09/2013 – 06/2017 Organized the selection and preparation of UC San Diego teams for the regional contest of ACM ICPC.
09/2006 – 06/2010 Represented University of Latvia in (sub)regional contests of ACM ICPC.

08/2006 18th International Olympiad in Informatics (IOI 2006) – bronze medal.
08/2005 17th International Olympiad in Informatics (IOI 2005) – silver medal.

05/2006 12th Baltic Olympiad in Informatics (BOI 2006) – bronze medal.
05/2005 11th Baltic Olympiad in Informatics (BOI 2005) – silver medal.
04/2004 10th Baltic Olympiad in Informatics (BOI 2004) – bronze medal.

Publications

[1] A. Kumar, J. Jaeger, and I. Stepanovs. "**Symmetric Signcryption and E2EE Group Messaging in Keybase**". To appear in: *EUROCRYPT 2024*. May 2024.

[2] M. R. Albrecht, L. Mareková, K. G. Paterson, and I. Stepanovs. "**Four Attacks and a Proof for Telegram**". In: *2022 IEEE Symposium on Security and Privacy*. May 2022. *Distinguished Paper Award.*

[3] M. Bellare and I. Stepanovs. "**Security Under Message-Derived Keys: Signcryption in iMessage**". In: *EUROCRYPT 2020, Part III*. Vol. 12107. LNCS. May 2020.

[4] 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*. May 2019.

[5] J. Jaeger and I. Stepanovs. "**Optimal Channel Security Against Fine-Grained State Compromise: The Safety of Messaging**". In: *CRYPTO 2018, Part I*. Vol. 10991. LNCS. Aug. 2018.

[6] M. Bellare, A. O'Neill, and I. Stepanovs. "**Forward-Security Under Continual Leakage**". In: *CANS 17*. Vol. 11261. LNCS. Nov. 2017.

[7] M. Bellare, A. C. Singh, J. Jaeger, M. Nyayapati, and I. Stepanovs. "**Ratcheted Encryption and Key Exchange: The Security of Messaging**". In: *CRYPTO 2017, Part III*. Vol. 10403. LNCS. Aug. 2017.

[8] M. Bellare, I. Stepanovs, and B. Waters. "**New Negative Results on Differing-Inputs Obfuscation**". In: *EUROCRYPT 2016, Part II*. Vol. 9666. LNCS. May 2016.

[9] M. Bellare and I. Stepanovs. "**Point-Function Obfuscation: A Framework and Generic Constructions**". In: *TCC 2016-A, Part II*. Vol. 9563. LNCS. Jan. 2016.

[10] M. Bellare, I. Stepanovs, and S. Tessaro. "**Contention in Cryptoland: Obfuscation, Leakage and UCE**". In: *TCC 2016-A, Part II*. Vol. 9563. LNCS. Jan. 2016.

[11] M. Bellare, I. Stepanovs, and S. Tessaro. "**Poly-Many Hardcore Bits for Any One-Way Function and a Framework for Differing-Inputs Obfuscation**". In: *ASIACRYPT 2014, Part II*. Vol. 8874. LNCS. Dec. 2014.

Further information

My web page provides the full information about my teaching experience, academic service, advising, and talks.