

Marcin Andrychowicz

Curriculum Vitae

Education

- 2013-2015 **PhD studies, Computer Science, University of Warsaw.**
I finished a 4-year PhD program in 2 years. My research concerned cryptocurrencies (e.g. Bitcoin) and cryptographic systems provably-secure against physical attacks.
- 2011-2013 **Master's Degree, Computer Science, University of Warsaw, GPA: 4.89/5.0.**
- 2008-2011 **Bachelor's Degree, Computer Science, University of Warsaw, GPA: 4.78/5.0.**
I have also studied Mathematics there for two years and Physics for one year.

Work experience

- 10.2015- **Research Scientist, GOOGLE DEEPMIND, London.**
05.2016 Working i.a. on memory architectures for neural networks.
- 02-07.2015 **Software Engineering Intern, GOOGLE INC., Warsaw, Poland.**
Working with the Brain team on applying *active learning* to neural networks.
- 04.2013 **Cryptographic audit, ZUNIT.COM, Warsaw, Poland.**
Auditing an electronic cash system.
- 07-09.2011 **Software Engineering Intern, GOOGLE INC., New York, U.S.**
Working on a next generation Google Maps prototype.
- 07-09.2010 **Software Engineering Intern, NVIDIA CORPORATION, Santa Clara, U.S.**
Accelerating and testing CUDA floating-point math library.
- 2008-2013 **Tutor, CENTER FOR INFORMATICS EDUCATION AND COMPUTER APPLICATIONS, Warsaw, Poland.**
Conducting regular classes for high school students interested in algorithms.

Publications

Machine Learning

- 2016 **Learning Efficient Algorithms with Hierarchical Attentive Memory,** M. Andrychowicz, K. Kurach
- 2015 **Neural Random-Access Machines, ICLR,** K. Kurach, M. Andrychowicz, I. Sutskever

Cryptography

- 2016 **Circuit Compilers with $O(1 / \log(n))$ Leakage Rate, EUROCRYPT,** M. Andrychowicz, S. Dziembowski, S. Faust
- 2015 **Secure Multiparty Computations on Bitcoin, Communications of the ACM,** M. Andrychowicz, S. Dziembowski, D. Malinowski, Ł. Mazurek.

Flat 1, 290 Caledonian Road, N1 1BA London

☎ (+44) 7438234128 • ✉ marcin.andrychowicz@gmail.com

1/3

- 2015 **PoW-Based Distributed Cryptography with no Trusted Setup**, *International Cryptology Conference (CRYPTO)*, M. Andrychowicz, S. Dziembowski
- 2015 **Leakage-Resilient Cryptography over Large Finite Fields: Theory and Practice**, *International Conference on Applied Cryptography and Network Security (ACNS)*, M. Andrychowicz, D. Masny, E. Persichetti
- 2015 **Efficient Leakage Resilient Circuit Compilers**, *RSA Conference Cryptographers' Track (CT-RSA)*, M. Andrychowicz, I. Damgaard, S. Dziembowski, S. Faust, A. Pournazeri
- 2015 **On the Malleability of Bitcoin Transactions**, *Second Workshop on Bitcoin Research (in Association with Financial Crypto)*, M. Andrychowicz, S. Dziembowski, D. Malinowski, Ł. Mazurek.
- 2014 **Modeling Bitcoin Contracts by Timed Automata**, *Formal Modeling and Analysis of Timed Systems (FORMATS)*, M. Andrychowicz, S. Dziembowski, D. Malinowski, Ł. Mazurek.
- 2014 **Fair Two-Party Computations via the Bitcoin Deposits**, *First Workshop on Bitcoin Research (in Association with Financial Crypto)*, M. Andrychowicz, S. Dziembowski, D. Malinowski, Ł. Mazurek.
- 2014 **Secure Multiparty Computations on Bitcoin**, *IEEE Symposium on Security and Privacy*, M. Andrychowicz, S. Dziembowski, D. Malinowski, Ł. Mazurek.

Patent applications

- 2016 **3 patent applications regarding Machine Learning techniques**.
Original assignee: Google Inc.
- 2012 **Circuit and method for identifying exception cases in a floating-point unit and graphics processing unit employing the same**, M. Andrychowicz, A. Fit-Florea.
Original assignee: NVIDIA Corporation.
The patent application concerns a universal method for accelerating computation of basic mathematical operations, which may be applied on software or hardware level and is currently used in GPUs with CUDA technology.

Books

- 2012 **Looking for a Challenge? The Ultimate Problem Set from the University of Warsaw Programming Competitions**, K. Diks (Ed.). Author of two chapters.

Awards

Scientific conferences

- 2014 **Best Paper Award** for the paper **Secure Multiparty Computations on BitCoin** on *IEEE Symposium on Security and Privacy 2014*.

Programming competitions

ACM-ICPC World Finals: bronze medal in 2009 and silver medal in 2013.
ACM-ICPC Central Europe Regional Contest (CERC): 1st place in 2008, 5th place in 2009 and 3rd place in 2012.

Polish Collegiate Programming Contest: 2nd place in 2009 and 2012.

TopCoder Open (Algorithm): finalist in 2012 and 2013.

TopCoder High School Finals: 3rd place in 2008.

International Olympiad in Informatics: gold medals in 2006, 2007 and 2008.

Central European Olympiad in Informatics: silver medal in 2006, bronze medal in 2007 and gold medal in 2008.

Baltic Olympiad in Informatics: gold medal in 2006.

Algorithmic Engagements: 1st place in 2008 and 3rd place in 2009.

Polish Olympiad in Informatics: silver medal in 2006, golds medals in 2007 and 2008.

Programming skills/languages

Fluent	C/C++ (including STL), LATEX, LUA (including TORCH)
Intermediate	JAVA, PYTHON, LINUX
Basic	HTML, JAVASCRIPT, PHP, SQL, ASSEMBLER, HASKELL, OCAML

Languages

fluent	English
intermediate	Russian
native	Polish