Mgr. Pavel Hubáček, Ph.D. *odborný asistent*

Kontaktní Informace

Informatický ústav Univerzity Karlovy,
Matematicko-fyzikální fakulta,
Malostranské nám. 25
118 00 Praha 1

hubacek@iuuk.mff.cuni.cz
http://hubacekpavel.wordpress.com

Výzkumné Zájmy

Teoretická informatika se zaměřením na kryptografii a její aplikace v teorii her a výpočetní složitosti.

Vzdělání

Aarhus University, Department of Computer Science, Denmark

Ph.D., Informatika, 2014

- Školitel: Prof. Jesper Buus Nielsen

Univerzita Karlova v Praze, Matematicko-fyzikální fakulta

Mgr., Matematické metody informační bezpečnosti, 2010

Bc., Obecná matematika, 2008

Odborná Praxe

Odborný asistent 01/2017 - současnost
Informatický ústav Univerzity Karlovy

Postdoctoral fellow 11/2016 - 08/2017
Foundations and Applications of Cryptographic Theory center,
Interdisciplinary Center, Herzliya, Israel
Host: Prof. Alon Rosen

Postdoctoral fellow 10/2014 - 10/2016
Department of Computer Science and Mathematics,
Weizmann Institute of Science, Rehovot, Israel
Host: Prof. Moni Naor

Visiting scholar 09/2013 - 02/2014
College of Computer and Information Science,
Northeastern University, Boston, MA
Host: Prof. Daniel Wichs

Research intern 09/2012 - 05/2013
Foundations and Applications of Cryptographic Theory Center,
IDC Herzliya, Israel
Host: Prof. Alon Rosen

Visiting student 09/2009 - 01/2010
Research Institute for Symbolic Computation,
Johannes Kepler University in Linz, Austria
Supervisor: Prof. Franz Winkler

Publikace ve Sbornících Recenzovaných Konferencí

1. Limits on the Power of Cryptographic Cheap Talk
   Pavel Hubáček, Jesper Buus Nielsen, Alon Rosen
   CRYPTO 2013 – 33rd International Cryptology Conference

2. Rational Arguments: Single Round Delegation with Sublinear Verification
   Siyao Guo, Pavel Hubáček, Alon Rosen, Margarita Vald
   ITCS 2014 – 5th Innovations in Theoretical Computer Science Conference

3. Cryptographically Blinded Games: Leveraging Players' Limitations for Equilibria and Profit
   Pavel Hubáček and Sunoo Park
   EC 2014 – 15th ACM Conference on Economics and Computation

4. On the Communication Complexity of Secure Function Evaluation with Long Output
   Pavel Hubáček and Daniel Wichs
   ITCS 2015 – 6th Innovations in Theoretical Computer Science

5. When Can Limited Randomness Be Used in Repeated Games?
   Pavel Hubáček, Moni Naor, Jonathan Ullman
   SAGT 2015 – 8th International Symposium on Algorithmic Game Theory

6. Rational Sumchecks
   Siyao Guo, Pavel Hubáček, Alon Rosen, Margarita Vald
   TCC 2016-A – 13th IACR Theory of Cryptography Conference

7. Hardness of Continuous Local Search: Query Complexity and Cryptographic Lower Bounds
   Pavel Hubáček and Eylon Yogev
   SODA 2017 – 28th ACM-SIAM Symposium on Discrete Algorithm

8. The Journey from NP to TFNP Hardness
   Pavel Hubáček, Moni Naor and Eylon Yogev
   ITCS 2017 – 8th Innovations in Theoretical Computer Science
   uděleno čestné pozvání (honorary invited paper)

Časopisecké Publikace

1. When Can Limited Randomness Be Used in Repeated Games?
   Pavel Hubáček, Moni Naor, Jonathan Ullman
   Theory of Computing Systems
   speciální vydání pro pozvané články z *SAGT 2014* a *SAGT 2015*

Stipendia

Postdoktorandský grant

- I-CORE ALGO postdoctoral scholarship – Israeli Center of Research Excellence in Algorithms. říjen 2014 - říjen 2016

Cestovní stipendium

- AKTION Česká republika - Rakousko. září 2009 - leden 2010

Odborné Prezentace

Cryptographic Cheap Talk

- China Theory Week 2012, Aarhus, Denmark 08/2012
- Greater Tel Aviv Area Cryptography Seminar, Ramat Gan, Israel 04/2013
- New Trends in Mechanism Design II Workshop, Aarhus, Denmark 06/2013
- CRYPTO 2013, Santa Barbara, CA 08/2013
- Northeastern University Theory Seminar, Boston, MA 10/2013

Rational Arguments

- China Theory Week 2013, Aarhus, Denmark 08/2013
- Boston University Security Seminar, Boston, MA 10/2013
- ITCS 2014, Princeton, NJ 01/2014
- MIT Cryptography and Information Security Seminar, Cambridge, MA 02/2014
- Harvard Economics and Computation Science Seminar, Cambridge, MA 02/2014
- Greater Tel Aviv Area Cryptography Seminar, Herzliya, Israel 05/2014
- Weizmann Institute Cryptography Reading Group, Rehovot, Israel 05/2014
- Bar-Ilan University Cryptography Reading Group, Ramat Gan, Israel 05/2014
- STTI 2015, Prague, Czech Republic 06/2015
- Weizmann Institute Theory Lunch Seminar, Rehovot, Israel 02/2016

Blinded Games

- Weizmann Institute Theory Lunch Seminar, Rehovot, Israel 11/2014
- Technion Game Theory Seminar, Haifa, Israel 12/2015

Communication Complexity in SFE with Long Output

- Greater Tel Aviv Area Cryptography Symposium, Tel Aviv-Yaffo, Israel 12/2014
- ITCS 2015, Rehovot, Israel 01/2015

Repeated Games with Limited Randomness

- HUJI Computation and Economics Seminar, Jerusalem, Israel 05/2015
- SAGT 2015, Saarbrücken, Germany 09/2015
- Greater Tel Aviv Area Cryptography Symposium, Herzliya, Israel 10/2015

Hardness of Continuous Local Search

- Symposium on Work of Ivan Damgård, Aarhus, Denmark 04/2016
- I-CORE Day 2016, Rehovot, Israel 04/2016
- HUJI Computation and Economics Seminar, Jerusalem, Israel 06/2016
- Weizmann Institute Theory Lunch Seminar, Rehovot, Israel 09/2016
- SODA 2017, Barcelona, Spain 01/2017

Profesionální Činost

Časopisecké recenze

- ACM Transactions on Economics and Computation
- Distributed Computing

Externí recenzent pro konference

- 2017: EUROCRYPT, CRYPTO, ICALP
- 2016: ITCS, EUROCRYPT, ICALP, FOCS, TCC-B, ASIACRYPT
- 2015: TCC, STOC, ASIACRYPT
- 2014: ICALP
- 2013: EUROCRYPT, TCC
- 2012: CRYPTO, PKC, TCC, CANS, Inscrypt
- 2011: CRYPTO, ASIACRYPT

Účast na konferencích a workshopech

- Greater Tel Aviv Area Cryptography Symposium, Rehovot, Israel 03/2017
- 7th Bar-Ilan Winterschool on Cryptography, Tel Aviv, Israel 02/2017
- Greater Tel Aviv Area Cryptography Symposium, Herzliya, Israel 01/2017
- SODA 2017, Barcelona, Spain 01/2017
- Greater Tel Aviv Area Cryptography Symposium, Ramat Gan, Israel 11/2016
- Greater Tel Aviv Area Cryptography Symposium, Tel Aviv, Israel 06/2016
- Bar-Ilan Workshop on Bitcoin, Ramat Gan, Israel 06/2016
- I-CORE Day 2016, Rehovot, Israel 04/2016
- Symposium on Work of Ivan Damgård, Aarhus, Denmark 04/2016
- Second Desert Workshop in Cryptography, Sde Boker, Israel 01/2016
- TCC 2016–A, Tel Aviv, Israel 01/2016
- 6th Bar-Ilan Winterschool on Cryptography, Tel Aviv, Israel 01/2016
- Greater Tel Aviv Area Cryptography Symposium, Tel Aviv, Israel 11/2015
- Greater Tel Aviv Area Cryptography Symposium, Herzliya, Israel 10/2015
- SAGT 2015, Saarbrücken, Germany 07/2015
- STTI 2015, Prague, Czech Republic 06/2015
- I-CORE Day 2015, Tel Aviv, Israel 04/2015
- 5th Bar-Ilan Winterschool on Cryptography, Tel Aviv, Israel 02/2015
- Greater Tel Aviv Area Cryptography Symposium, Rehovot, Israel 02/2015
- Greater Tel Aviv Area Cryptography Symposium, Ramat Gan, Israel 01/2015
- ITCS 2015, Rehovot, Israel 01/2015
- Greater Tel Aviv Area Cryptography Symposium, Tel Aviv-Yaffo, Israel 12/2014
- Greater Tel Aviv Area Cryptography Symposium, Tel Aviv, Israel 11/2014
- Theory and Practice of Secure MPC Workshop, Aarhus, Denmark 05/2014
- ITCS 2014, Princeton, NJ 01/2014
- New York CS and Economics day, New York, NY 10/2013

- Faces of Modern Cryptography, New York, NY 10/2013
- CRYPTO 2013, Santa Barbara, CA 08/2013
- China Theory Week 2013, Aarhus, Denmark 07/2013
- New Trends in Mechanism Design II Workshop, Aarhus, Denmark 06/2013
- Modeling Intractability Workshop, Mitzpe Ramon, Israel 02/2013
- 3rd Bar-Ilan Winterschool on Cryptography, Tel Aviv, Israel 02/2013
- China Theory Week 2012, Aarhus, Denmark 08/2012
- Theory and Practice of Secure MPC Workshop, Aarhus, Denmark 06/2012
- 2nd Bar-Ilan Winterschool on Cryptography, Tel Aviv, Israel 02/2012
- China Theory Week 2011, Aarhus, Denmark 10/2011
- New Trends in Mechanism Design Workshop, Copenhagen, Denmark 09/2011
- Innovations in Algorithmic Game Theory Workshop, Jerusalem, Israel 05/2011
- EUROCRYPT 2011, Talin, Estonia 05/2011
- Workshop on Solution Concepts for Extensive Games, Aarhus, Denmark 06/2010

Pedagogická Praxe

Organizace seminářů - Department of Computer Science and Applied Mathematics, Weizmann Institute of Science

Bitcoin Seminar léto 2016
Seminář o kryptografických měnách organizovaný spolu s Prof. Moni Naorem.

Weizmann Cryptography Group Seminar zima 2014 – léto 2016
Výzkumný seminář o nových výsledcích v kryptografii.

Vedení cvičení - Department of Computer Science, Aarhus University

Optimization (dOpt) léto 2011 a 2012
Přednášející: Prof. Peter Bro Miltersen and Prof. Kristoffer Arnsfelt Hansen

Combinatorial Search (dKS) léto 2011 a 2012
Přednášející: Prof. Peter Bro Miltersen and Prof. Kristoffer Arnsfelt Hansen

Introductory Programming (dIntProg) zima 2011
Přednášející: Aino Vonge Corry, Ph.D. and Prof. Michael Edelgaard Caspersen

Programming 2 (dProg2) zima 2011
Přednášející: Gudmund Skovbjerg Frandsen, Ph.D.