Marko Horvat

Radno iskustvo

2018.— **Poslijedoktorand**, *Prirodoslovno-matematički fakultet, Matematički odsjek (PMF-MO)*, Zagreb, Hrvatska.

Vježbe: *Diskretna matematika, Teorija skupova, Programiranje 1, Programiranje 2, Strukture podataka i algoritmi, Baze podataka*

Predavanja: *Interpretacija programa*

Tajnik *Seminara za matematičku logiku i osnove matematike*

Projekt: Izračunljive strukture, odlučivost i složenost

2016.–2018. **Poslijedoktorand**, *Max Planck Institute for Software Systems (MPI-SWS)*, Kaiserslautern, Njemačka.

Teorija složenosti (zamjenski predavač), *Teorija konkurentnosti* (gost predavač)

Projekt: imPACT

2014. **Asistent i znanstveni novak**, *University of Oxford*, Oxford, UK.

Napredna sigurnost (vježbe i praktikum)

2011.–2013. **Asistent i znanstveni novak**, *ETH Zürich*, Zürich, Švicarska.

Informacijska sigurnost, Diskretna matematika

Projekt: Security protocol improvement and adversary change

2010. **Asistent**, *Fakultet elektrotehnike i računarstva*, Zagreb, Hrvatska.

Matematika II

2007. **Demonstrator**, *PMF-Matematički odjel*, Zagreb, Hrvatska.

Matematička logika

Obrazovanje

2013.–2016. **Doktorski studij računarstva**, *Department of Computer Science, University of Oxford*, Oxford, UK.

Doktorski rad: *Formal analysis of modern security protocols in current standards*

2011.–2013. **Doktorski studij računarstva, smjer Informacijska sigurnost**, *Department of Computer Science, ETH Zürich*, Zürich, Švicarska.

Položeni kolegiji: *Formalne metode u informacijskoj sigurnosti*, *Razvoj formalnih sustava*, *Kriptografija*

2010.–2011. **Doktorski studij matematike**, *PMF-Matematički odsjek, Sveučilište u Zagrebu*, Zagreb, Hrvatska.

Odslušani kolegiji: *Logika i računarstvo*, *Teorija, metodike i povijest infinitezimalnih računa*, *Teorija modela modalne logike*, *Primijenjena logika*

2004.–2010. **Diplomski studij matematike, smjer Teorijska matematika**, *PMF-Matematički odjel, Sveučilište u Zagrebu*, Zagreb, Hrvatska.

Diplomski rad: *Goldblatt-Thomasonov teorem*

Prosjek: 4.795

Zagreb, Hrvatska
mhorvat@math.hr

Znanstveni interesi

Logika u računarstvu

- Modeliranje i verifikacija kompleksnih sustava (distribuirani, kiber-fizički, itd.)
- Osnove matematike i računarstva

Matematika u računarstvu

- Kriptografija i teorija brojeva
- Izračunljiva topologija

Sigurnost

- Informacijska sigurnost (posebno sigurnosni protokoli)
- Mrežna sigurnost
- Sistemska sigurnost

Popis radova

Priopćenja na konferencijama

[1] Cas Cremers, Marko Horvat, Jonathan Hoyland, Sam Scott i Thyla van der Merwe. "A Comprehensive Symbolic Analysis of TLS 1.3". *Proceedings of the 24th ACM Conference on Computer and Communications Security*. ACM, 2017, str. 1773–1788.

[2] Cas Cremers, Marko Horvat, Sam Scott i Thyla van der Merwe. "Automated Analysis and Verification of TLS 1.3: 0-RTT, Resumption and Delayed Authentication". *Proceedings of the 37th IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2016, str. 470–485.

[3] Cas Cremers i Marko Horvat. "Improving the ISO/IEC 11770 Standard for Key Management Techniques". *Proceedings of the 1st International Conference on Security Standardisation Research (SSR 2014)*. Sv. 8893. Lecture Notes in Computer Science. Springer, 2014, str. 215–235.

[4] David Basin, Cas Cremers i Marko Horvat. "Actor Key Compromise: Consequences and Countermeasures". *Proceedings of the 27th IEEE Computer Security Foundations Symposium (CSF 2014)*. 2014, str. 244–258.

[5] Vedran Čačić, Marko Doko, Marko Horvat i Domagoj Vrgoč. "Changing the order of summation for series beyond ω [sažetak]". *2009 European Summer Meeting of the Association for Symbolic Logic Logic Colloquium '09*. Sv. 16. 1. 2010, str. 90–142. URL: `http://www.jstor.org/stable/25614512`.

Radovi u časopisima

[6] Vedran Čačić, Marko Doko i Marko Horvat. "Rearranging absolutely convergent well-ordered series in Banach spaces". *Rad HAZU, Matematičke znanosti* 23.538 (2019).

[7] Jyotirmoy Deshmukh, Marko Horvat, Xiaoqing Jin, Rupak Majumdar i Vinayak S. Prabhu. "Testing Cyber-Physical Systems Through Bayesian Optimization". *ACM Transactions on Embedded Computing Systems* 16.5s (2017), str. 1–18. URL: `http://doi.acm.org/10.1145/3126521`.

[8] Cas Cremers i Marko Horvat. "Improving the ISO/IEC 11770 standard for key management techniques". *International Journal of Information Security* 15.6 (2015), str. 659–673. URL: `http://dx.doi.org/10.1007/s10207-015-0306-9`.

Konferencijska predavanja i seminari

- *Rearranging absolutely convergent well-ordered series in Banach spaces*, Logic and Applications, 27.09.2019., Dubrovnik, Hrvatska
- *Rearranging absolutely convergent well-ordered series in Banach spaces*, Logic Colloquium, 16.08.2019., Prag, Češka
- *Verifying security protocols with Tamarin*, Systematic Analysis of Security Protocol Implementations, 15.06.2018., Leiden, Nizozemska
- *Uspjesi formalne verifikacije u standardizaciji sigurnosnih protokola*, znanstveni kolokvij, 09.05.2018., PMF-MO
- *Testing Cyber-Physical Systems through Bayesian Optimization*, EMSOFT 2017, 16.10.2017., Seoul, Južna Koreja
- *Automated Analysis and Verification of TLS 1.3: 0-RTT, Resumption and Delayed Authentication*, IEEE Symposium on Security and Privacy 2016, 24.05.2016., San Jose, CA, SAD
- *Automated Analysis and Verification of TLS 1.3: 0-RTT, Resumption and Delayed Authentication*, CryptoAction Symposium, 07.04.2016., Budimpešta, Mađarska
- *Automated Analysis of TLS 1.3*, Seminar za matematičku logiku i osnove matematike, 04.04.2016., PMF-MO
- *Hardening current (and future) security protocol standards*, 10.02.2016., MPI-SWS, Kaiserslautern, Njemačka
- *Hardening current (and future) security protocol standards*, RiSE Seminar, 26.11.2015., IST Austria, Klosterneuburg, Austrija
- *Razbijanje modernih protokola pomoću računala (2)*, Seminari za teorijsko računarstvo/logiku i osnove matematike, 19.10.2015., PMF-MO
- *Razbijanje modernih protokola pomoću računala*, Seminari za teorijsko računarstvo/logiku i osnove matematike, 14.09.2015., PMF-MO
- *Improving the ISO/IEC 11770 standard for key management techniques*, SSR 2014, 16.12.2014., London, UK
- *Improving the ISO/IEC 11770 standard for key management techniques*, Seminar za matematičku logiku i osnove matematike, 24.11.2014., PMF-MO
- *Actor Key Compromise: Consequences and Countermeasures*, CSF 2014, 21.07.2014., Beč, Austrija
- *Sigurnost nakon gubitka ključeva*, Seminar za matematičku logiku i osnove matematike, 30.09.2013., PMF-MO
- *Protokoli od A do B*, Seminar za matematičku logiku i osnove matematike, 11.04.2012., PMF-MO
- *The Goldblatt-Thomason theorem*, 10.06.2011., ETH Zürich, Zürich, Švicarska
- *The Goldblatt-Thomason theorem/The size-change termination principle*, 10.06.2011., Technische Universität Wien, Beč, Austrija
- *The Goldblatt-Thomason theorem (diplomski seminar)*, Seminar za matematičku logiku i osnove matematike, 04.10.2010., PMF-MO

Suradnja s tvrtkama

2017. **Toyota**.
Korištenje Bayesove optimizacije u testiranju prototipova raznih kiber-fizičkih sustava

2015.–2016. **Mozilla**.
Službeni TLS 1.3 contributor (`https://tools.ietf.org/html/rfc8446`)

Ostalo obrazovanje i konferencije

2017. Computer and Communications Security (CCS), Dallas, TX, SAD

Computer Aided Verification (CAV), Heidelberg, Njemačka

Chaos Communication Congress (putem web-streama, od 2010.), Berlin, Njemačka

2016. Real World Cryptography (dodijeljen travel award), Stanford, CA, SAD

2015. IETF 93 (putem web-streama), Prag, Češka

2014. ACM WiSec 2014 (Wireless Security), Oxford, UK

Design and security of cryptographic algorithms and devices for real-world applications (dodijeljen travel award), Šibenik, Hrvatska

2012. Logic Colloquium 2012, Manchester, UK

2011. European Summer School in Logic, Language and Information (ESSLLI), Ljubljana, Slovenija

2010. Logic Colloquium 2010 (dodijeljen travel award), Pariz, Francuska

Teorija modela i primjene (trodnevni seminar, I. Tomašić), Zagreb, Hrvatska

2009. Napredna teorija skupova (kratak kurs, M. Džamonja), Zagreb, Hrvatska

3rd Free Software Festival, Čakovec, Hrvatska

2007. 3rd Bite-On Security, Zagreb, Hrvatska

Stipendije

Engineering and Physical Sciences Research Council stipendija

Stipendija grada Samobora za nadarene studente

Računalne vještine

Formalna verifikacija: Tamarin, Scyther

Obrada makroa: m4

Statistika: MATLAB

Programski jezici: Perl, Python, C

Prijelom: LaTeX, MetaPost, PGF/TikZ

Version control: git, SVN

Strani jezici

Engleski (aktivno poznavanje), njemački (aktivno poznavanje u pismu, pasivno u govoru), francuski (pasivno poznavanje)