

Strukturovaný profesní životopis



Jméno: prof. Ing. Róbert Lórencz, CSc.
Bydliště: Pátecká 1384, 290 01 Poděbrady
E-mail: lorencz@cvut.cz

Datum narození	10. 8. 1957, Prešov
Vzdělání	2012 prof. – oboru Informatika a výpočetní technika na FIT VUT Brno 2005 doc. – obor Výpočetní technika a informatika (habilitační práce: „New Approaches to Computing the Modular Inverse in Hardware“) 1985 – 1990 CSc. – obor Meracia a výpočtová technika (Bezchybové numerické riešenie dekonvolúcie a dekompozície spektier v jadrovej fyzike), Ústav merania a meracej techniky SAV Bratislava 1976 – 1981 Ing. – FEL ČVUT Praha, obor Sdělovací elektrotechnika, specializace Teorie elektromagnetického pole (Dolnofrekvenční mikro-pásková propust)
Dosavadní praxe	2013 – dosud FIT ČVUT, profesor, vedoucí Katedry počítačových systémů (od 2015 - 2018), vedoucí Katedry informační bezpečnosti (KIB) (od 2018) 2009 – 2013 FIT ČVUT, profesor, vedoucí Katedry počítačových systémů, proděkan pro VaV 1998 – 2009 FEL ČVUT, Katedra počítačů, odborný asistent, zástupce vedoucího katedry 1995 – 1996 FEI TU Košice, katedra počítačů, odborný asistent 1992 – 1995 Škoda auto a.s. Mladá Boleslav, systémový analytik 1983 – 1989 Fyzikální ústav SAV Bratislava, vědeckovýzkumný pracovník 1982 – 1983 Nukleární centrum KU Praha, studijní pobyt
Zahraníční pobyty	1996 – 1998 Deutsches Elektronen-Synchrotron DESY Hamburg, vědeckovýzkumný pracovník 1990 – 1991 Ludwig Maximilians-Universität Mnichov, vědeckovýzkumný pracovník, působiště: GSI (Gesellschaft für Schwerionenforschung) Darmstadt
Výzkum	Oblast výzkumu: kryptografie a kryptoanalýza, bezpečnost počítačových systémů a sítí, kybernetická bezpečnost, numerické algoritmy, detekce malware Členství: vedoucí výzkumné skupiny Aplikovaná numerická matematika a kryptologie, člen vědecké rady FIT a FIIT STU v Bratislave
Pedagogika	Garant bakalářského programu Informatika, Garant studijní specializace Bezpečnost a informační technologie v bakalářském studijním programu Informatika a garant studijní specializace Bezpečnost v magisterském studijním programu Informatika. Školitel doktorandů: 9 obhájených a 7 studujících. Vedoucí víc než 30 obhájených mag. závěrečných prací a víc než 20 obhájených bak. prací. Přednášející a garant předmětů: Pokročilá kryptologie (mag.), Kryptologie a bezpečnost (bak.), Aplikovaná numerická matematika (dok.), Vestavná bezpečnost (dok.)
Členství v komisích	Programové výbory: více než 40krát člen programových komisí mezinárodních konferencí, více než 30krát jiných konferencí Členství: člen redakční rady časopisu “Bulletin of the ACM Slovakia” (2011 – 2020), senior člen “CryptArchi Club” (2006 –) Věd. rada: FEL ČVUT v Praze (2012 – 15), FIT ČVUT v Praze (2009 –), FIIT STU v Bratislavě (2020 –)
Ostatní aktivity	Soudní znalec z oboru kybernetika odvětví výpočetní technika se specializací výpočetní a komunikační technika, informatiku, bezpečnost informačních systémů a sítí a kryptologie, a dále v oboru kriminalistika se specializací bezpečnost informačních systémů a sítí, ochrana dat, kriminalistickou počítačovou expertizu, kybernetiku. Člen Výboru pro kybernetickou bezpečnost na ČVUT (2021-25), člen správní rady zapsaného ústavu CyberSecurity Hub, z.ú. (2022 –)
Publikační činnost	>50 časopiseckých článků, >70 peer-reviewed konferenčních příspěvků, 2 národní patenty, 1 US patent., 230 WoS citací (bez auto-citací, víc než 680GS citations, WoS H-index = 10 (bez auto-citací 8), Scopus H-index = 10, Scholar H-index = 14.
Vybrané publikace	<i>Časopisecké články:</i> 1. Jurečková, O.; Jureček, M.; Stamp, M.; Di Troia, F.; Lórencz, R.: Classification and online clustering of zero-day malware. Journal of Computer Virology and Hacking Techniques, 2024, 1-14.

2. Rabas, T.; Buček, J.; Lórencz, R.: Single-Trace Side-Channel Attacks on NTRU Implementation. *SN Computer Science*, 2024, 5(2), 239.
3. Kokeš, J.; Matějka, J.; Lórencz, R.: Automatic Detection and Decryption of AES Using Dynamic Analysis. *SN Computer Science*, 2022, 3(5), 338.
4. Kodýtek, F.; Lórencz, R.; Buček, J.: Three counter value based ROPUFs on FPGA and their properties. *Microprocessors and Microsystems*, 2022, 88, 1-10. ISSN 0141-9331. DOI 10.1016/j.micpro.2021.104375.
5. Jureček, M.; Lórencz, R.: Application of Distance Metric Learning to Automated Malware Detection. *IEEE Access*, 2021, 9, 96151-96165.
6. Jureček, M.; Lórencz, R.: Malware Detection Using a Heterogeneous Distance Function. *Computing and Informatics*, 2018, 37(3), 759-780.
7. Buchovecká, S.; Lórencz, R.; Kodýtek, F.; Buček, J.: True random number generator based on ring oscillator PUF circuit. *Microprocessors and Microsystems*, 2017, 53(0), 33-41. ISSN 0141-9331.
8. Buček, J.; Kubalík, P.; Lórencz, R.; Zahradnický, T.: Design of a Residue Number System Based Linear System Solver in Hardware. *Journal of Signal Processing Systems*, 2017, 87(3), 343-356.
9. Kodýtek, F.; Lórencz, R.; Buček, J.: Improved ring oscillator PUF on FPGA and its properties. *Microprocessors and Microsystems*, 2016, 47, 55-63.
10. Kodýtek, F.; Lórencz, R.: Proposal and Properties of Ring Oscillator-Based PUF on FPGA. *Journal of Circuits Systems and Computers*, 2016, 25(3).
11. Lórencz, R.; Hlaváč, J.: Subtraction-free Almost Montgomery Inverse algorithm. *IPL*, 2005, 94(1), 11-14. ISSN 0020-0190.
12. Lórencz, R.; Wagner, V.; Kugler, A.; Pachr, M.; Šumbera, M. et al.: Detection of Relativistic Neutrons by BaF2 Scintillators. *Nuclear Instruments and Methods in Physics Research, Section A*, 1997, 50(A 394), 332-340. ISSN 0168-9002.
13. Lórencz, R.; Kugler, A.; Wagner, V.; Pachr, M.; Šumbera, M. et al.: Emission of Nucleons and Light Fragments Relative to Reaction Plane in Bi+Pb Collisions at 1 GeV/u. *Physics Letters B*, 1994, 3-4(B 335), 319-325. ISSN 0370-2693.
14. Lórencz, R.; Morháč, M.: Modular System for Solving Linear Equations Exactly, II. Hardware Realization and Firmware. *Computing and Informatics*, 1992, 11(4), 497-507. ISSN 1335-9150.
15. Lórencz, R.; Berg, F.D.; Boonstra, A.; Braak, H.P.; Brummund, N. et al.: Neutral Meson Production in Relativistic Heavy Ion Collision. *Zeitschrift fur Physik A: Hadrons and Nuclei*, 1991, 20(340), 297-302. ISSN 0939-7922. Now EUROPEAN PHYSICAL JOURNAL A, ISSN 1434-6001.

Konferenční příspěvky:

1. Holec, M.; Lórencz, R. et al.: X-Ray Radiation Effects on SRAM-Based TRNG and PUF. In: *Proceedings of the 11th International Conference on Information Systems Security and Privacy*. International Conference on Information Systems Security and Privacy, Porto, 2025-02-20/2025-02-22. Setúbal: Science and Technology Publications, Lda, 2025. s. 375-384. sv. 2. ISSN 2184-4356. ISBN 978-989-758-735-1. DOI [10.5220/0013314100003899](https://doi.org/10.5220/0013314100003899). Dostupné z: <https://www.scitepress.org/PublicationsDetail.aspx?ID=7qLQgHcFBVQ=&t=1>
2. Staníček, O.; F. Kodýtek a R. Lórencz: Counter power leakage for frequency extraction of ring oscillators in ROPUF. In: KRYJAK, T. a F. PÉTROU, eds. *Proceedings of the 2024 27th Euromicro Conference on Digital System Design*. 27th Euromicro Conference Series on Digital System Design, Paris, 2024-08-28/2024-08-30. Los Alamitos: IEEE Computer Society, 2024. s. 26-32. ISSN 2771-2508. ISBN 979-8-3503-8038-5.
3. Rabas, T.; Buček, J.; Lórencz, R.: Single-Trace Attack on NTRU Decryption with Machine Learning and Template Profiling. 2023 26th Euromicro Conference on Digital System Design (DSD), 2023, 124-129.
4. Rabas, T.; Buček, J.; Lórencz, R.: SPA Attack on NTRU Protected Implementation with Sparse Representation of Private Key. *ICISSP*, 2023, 135-143.
5. Kokeš, J.; Lórencz, R.: On the Use of Multiple Approximations in the Linear Cryptanalysis of Baby Rijndael. 2023.
6. Kotlaba, L.; Buchovecká, S.; Lórencz, R.: Active Directory Kerberoasting Attack: Detection using Machine Learning Techniques. *ICISSP 2021*, s. 376-383.

7. Jureček, M.; Jurečková, O.; Lórencz, R.: Improving classification of malware families using learning a distance metric. Int. Conf. on Information Systems Security and Privacy - ICISSP 2021, s. 643-652.
8. Kokeš, J.; Matějka, J.; Lórencz, R.: Automatic Detection and Decryption of AES by Monitoring S-Box Access. ICISSP 2021, s. 172-180.
9. Kodýtek, F.; Lórencz, R.; Buček, J.: Comparison of three counter value based ROPUFs on FPGA. In: Proceedings of the 23rd Euromicro Conference on Digital Systems Design, Virtual Event organized from Kranj, Slovenia, 2020-08-26/2020-08-28. Los Alamitos, CA: IEEE Computer Soc., 2020, s. 205-212.
10. Kotlaba, L.; Buchovecká, S.; Lórencz, R.: Active Directory Kerberoasting Attack: Monitoring and Detection Techniques. In: Proceedings of the 6th International Conference on Information Systems Security and Privacy, Valletta, 2020-02-25/2020-02-27. Madeira: SciTePress, 2020, s. 432-439.
11. Jureček, M.; Lórencz, R.: Distance Metric Learning using Particle Swarm Optimization to Improve Static Malware Detection. In: Proceedings of the 6th International Conference on Information Systems Security and Privacy. Valletta, 2020-02-25/2020-02-27. Madeira: SciTePress, 2020, s. 725-732.
12. Buchovecká, S.; Lórencz, R.; Buček, J.; Kodýtek, F.: Lightweight Authentication and Secure Communication Suitable for IoT Devices. ICISSP 2020, s. 75-83.
13. Jureček, M.; Buček, J.; Lórencz, R.: Side-Channel Attack on the A5/1 Stream Cipher. DSD 2019, s. 633-638.
14. Buchovecká, S.; Lórencz, R.; Kodýtek, F.; Buček, J.: True Random Number Generator Based on ROPUF Circuit. In: Proceedings of 19th Euromicro Conference on Digital System Design DSD 2016. Limassol, Cyprus, 31.08.2016 - 02.09.2016. Los Alamitos, CA: IEEE Computer Soc., 2016, s. 519-523.

Patenty:

1. Lórencz, R.: Method for Generating the Multiplicative Inverse in a Finite Field $GF(p)$. Patent United States Patent and Trademark Office, 7574469. 2009-08-11.
2. Lórencz R.: Způsob generování multiplikativní inverze nad konečným tělesem $GF(p)$, Patent Úřad průmyslového vlastnictví, 294898. 2005-02-07, 2005.
3. Morháč, M. - Lórencz, R.: Architektúra procesorovej jednotky. Patent Úřad průmyslového vlastnictví, 257355. 1987-05-14.

Vybrané granty

1990 – 1991	TAPS projekt, GSI Darmstadt, Německo (člen řešitelského týmu).
1996 – 1998	Extrakce parametrů pomoci SPICE modelů, FEC DESY, Německo (řešitel).
2002 – 2003	Spolupráce odborných vysokých škol v boji státu s počítačovou kriminalitou. Nejzávažnější bezpečnostní rizika, grant MV ČR (člen řešitelského týmu).
2005 – 2011	Výzkumný záměr, Výzkum perspektivních informačních a komunikačních technologií, (člen řešitelského týmu v kategorii D1).
2007 – 2010	Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů ČR, grant MV ČR (spoluřešitel).
2012 – 2014	Studium vlastností residuální aritmetiky pro řešení SLR, GA ČR, (řešitel).
2012 – 2016	ICT COST Action IC1204, Trustworthy Manufacturing and Utilization of Secure Devices, TRUDEVICE, (člen řídicího výboru za ČR)
2016 – 2018	Výzkum vztahů a společných vlastností spolehlivých a bezpečných architektur založených na programovatelných obvodech, (člen řešitelského týmu)
2018 – 2022	Bezpečnost a zabezpečení jaderných zařízení a forenzní analýzy jaderných materiálů CVUT-NSSF, studijní program a laboratoř, řešitel na FIT.
2018 – 2022	RCI - Výzkumné centrum informatiky, vedoucí programu Bezpečnost vestavných systémů.
2023 – 2025	EDIH

V Praze, dne 24. 4. 2025

prof. Ing. Róbert Lórencz, CSc.