RESUME – Laszlo Hars, PhD

Boeing Technical Fellow

Summary

For decades I led and practiced R&D in many fields, including *Information Security: Cryptography, Anti Tamper*; *Systems Architecture, Applied Mathematics, Machine Learning, Artificial Intelligence, Algorithm Development* and *Optimizations*. I was the chief cryptographic architect of Boeing's secure microprocessors, Seagate's Self Encrypting- and Solid-State Drives, and Panasonic's digital rights management and document archiving systems. I also led projects in *measurements, modeling, simulations* and *electronic design*, as well as performed research and lectured at universities in *mathematics* and *computer science*. I was responsible for setting strategic directions of companies; project schedule, resource allocation and risk management; defined project lines; selected, trained and appraised team members, supervised Ph.D. students and interns.

I hold active **Top Secret / SCI** DoD security **clearance**.

I authored 66 granted **patents**, 100+ patent applications, and 50 technical **publications**.

I retired from Boeing in July, 2021, but I am considering getting back to work.

Degrees, Education

- **Ph.D.** in Mathematics (*Computational Geometry*)
  (Eötvös Loránd University, Budapest, 1977. Thesis: Density of Circle Packings)
- **M.Sc.** in *Computer Science*
  (Eötvös Loránd University, Budapest 1975. Thesis: Complexity of Algorithms)
- **Diploma** in Economics (ML University, Budapest 1978.)
- **Post-doc scholarship**: Networked systems (Kyoto University, 1979-81)

Selected Projects

- Information Protection in computing and storage devices: Security architectures, Information assurance, Anti tamper (AT), Bit-mixers, Ciphers, Hash functions, Protocols – Design, Applications and Implementations
- Random number generators (RNG): Electronic entropy sources; Randomness tests
- Physical Unclonable Functions (PUF): Physical sources; Assessments
- Quantum computing: Post-Quantum cryptography
- Measurements: Design and Construction of Electronic Hardware and Software
- Medical: Design and Construction of instruments, Treatment planning
- Machine learning (ML), Artificial Intelligence (AI)
- Data science, modelling, simulations
- Discrete and Large-scale Optimizations, Control
- Software development: Security systems, Digital Signal Processing (DSP)
- Mathematics: Operations Research, Complexity of Algorithms, Graph theory, Discrete geometry, Number theory, Numerical methods and Abstract algebra

Experiences

INFORMATION SECURITY	***Security Systems Architecture*** ***Cryptography*** Security systems architectures; Threat models. Designed, implemented and optimized *Cryptosystems*; *Cryptographic Toolboxes*; Long *arithmetic* methods; Communication *protocols*, Encryption *modes*, *Bit mixers*, *RAX Ciphers* ***Anti-Tamper (AT)*** analyzed, devised and evaluated physical attacks on information systems, developed countermeasures ***Tamper Resistant SW*** improved known techniques, invent new ones ***Random Number Generators*** designed new ones, improved old ***Random Number Tests*** analyzed and improved tests, designed new ones ***Physical Unclonable Functions*** designed, analyzed; investigated sources ***Copyright Management***, ***Copy Protection, Software obfuscation*** invented, analyzed and programmed new methods ***Digital Watermarking*** developed new methods (audio, image, document), applied signal processing for test and evaluation; investigated attacks
ELECTRICAL ENGINEERING R & D	***Signal Quality Measurement*** Designed and built instruments for spread spectrum telecommunication systems (CDMA, GSM, DECT, NADC) ***Signal Generation*** Designed and built instruments for very low distortion, wide-band modulated signals ***Electronic Systems Modeling*** Mathematical analysis and system simulations (noise effects, distortion, phase jitter, frequency drift, ADC resolution − quantization errors, rounding errors …) ***Circuits Design*** New algorithms for analog and digital filter design and implementation; randomness source, data recorder, demodulator, power supply and many other circuits ***Spectrum Analyzers*** Designs and constructions (sweeping- and FFT-based) ***Digital Oscilloscopes*** Design and construction; Novel Calibration Methods
SOFTWARE DEVELOPMENT	***Systems Modeling*** Simulations of complex systems ***Digital Signal Processing*** DSP software, new methods and signal analyses ***Instrument Control*** Architectures and SW development ***Mathematical SW*** Designed and programed *Graph* creating and manipulating packages, equations *Editor*, *Planar Drawing* of graphs, Simultaneous Rational Approximations, Truncated arithmetic ***Parallelization*** of network-, sorting- and matrix-algorithms ***Compiler*** design and ***Language*** definition for a list manipulation language ***Medical Systems*** Modeling, SW design: dosage of *antibiotic treatment*, model of *concentration* of chemicals and decomposition products in the blood; *Dialysis Planning* at severe kidney insufficiency ***Routing*** New algorithms and SW for VLSI design, multi-chip modules ***Control*** SW and algorithms for component placements, routing ***Utilities*** Electronic Musical Instruments and I/O devices for the disabled ***Statistical*** Estimation and Evaluation of measurements ***Combinatorial Games*** algorithms and programs

DATA SCIENCE	***Machine Learning*** (ML), ***Artificial Intelligence*** (AI), ***Data Mining***, ***Modelling***, ***Simulations***: implemented, developed new methods
UNIVERSITY LECTURING	***UNDERGRADUATE COURSES***: Geometry, Calculus, Combinatory, Combinatorial Games, Graph Theory, Computer programming ***GRADUATE COURSES***: Differential Geometry, Non-Euclidean Geometries, Discrete Geometry, Algorithmic Theory, Combinatorial Algorithms, Numerical Methods, Computational Geometry, Parallel processes, Data Structures
BASIC RESEARCH	***Special Functions*** Crypto applications, invertibility; Fermat numbers ***Computational Geometry*** new algorithms for numerical best placements of objects on surfaces of constant curvature (cookie-cutter problems) ***Computer Graphics*** Designed, analyzed fast second order *curve drawing methods;* data structures and algorithms for planar projections of 3D bodies ***Discrete Geometry*** Solved open problems about *optimal placements* of objects on surfaces; Studied *Equivalence classes* of polyhedra by dissection ***Complexity of Algorithms*** (geometric, numeric, combinatorial) ***Optimizations*** Geometric, numeric and combinatorial algorithms ***Numerical Methods*** Long integer arithmetic, differential equations, roots of polynomials / smooth functions, special functions, matrix calculations ***Discrete Orthogonal Transformations*** speed-ups, new algorithms ***Networks*** File allocation and traffic optimizations ***VLSI Design*** Placement-, wire routing algorithms

Tools Mastered

- SW Applications: MATLAB, Maple, Wolfram Mathematica, MS Office, VISIO…
- Operating Systems: MS Windows, Unix/Linux, RTOS
- Programming Languages: Assembler (DSP, x86, ARM), C/C++, AHK, Python, Julia, Java, Verilog, VHDL
- Analog and digital *measurement* systems

Professional Activities

- Boeing's representative in 4 workgroups of TCG (Trusted Computing Group) 2014-2016
- Regular reviewer of scientific papers submitted for publication in international scientific journals (2014: Top Reviewer Award of IEEE Transactions on Computers)
- Program committee member: CHES 2006
- Panelist, National Science Foundation review of Cyber Trust (ISG) proposals (2005)
- Member of 4 IEEE P1619 (Security In Storage) standards committees (2004 - 2011)
- Organizer, chairman of the Philips Information Security Workshop (2001, Eindhoven)
- Coordinator of the Parallel Processing group, Eötvös Loránd University (1987−1989)
- Chairman of the National High-School Mathematical Contest committee (1984−1988)

Work Experiences

5/2011 – 7/2021	**Boeing SCS <- CPU Technology, Inc.** 5753 W. Las Positas Blvd. Pleasanton CA 94588-4084	*Chief Cryptographic Architect* System design, RNGs, PUFs, InfoSec, AT, Cryptography, Secure HW
9/2002 – 5/2011	**Seagate Technology** 389 Disc Drive Longmont, CO 80503	*Principal Engineer-Scientist* Manage R&D projects System design, RNGs, InfoSec, Crypto
2/2000 – 8/2002	**Philips Research, USA** 345 Scarborough Rd Briarcliff Manor, NY 10510	*Senior/Lead Scientist* Lead research projects Random Numbers, InfoSec, DRM
7/1998 – 2/2000	**Panasonic Technologies, Inc.** Panasonic Information and Networking Technologies Laboratory, Princeton, NJ	*Senior/Lead Scientist* Lead research projects Digital Watermarking, Cryptography
1/1990 – 6/1998	**Schlumberger Technologies – Wavetek Corp**. Ismaning, Germany	*Chief Technologist* Mathematics and Simulations, Software, Electronic Design, R&D Management
6/1988 – 1/1990	Institute for Operations Research **University Bonn,** Bonn, Germany	*Visiting researcher* VLSI design, Large Scale Optimizations
8/1985 – 9/1992	Dept. of Computer Science **Eötvös Loránd University** Budapest, Hungary	*Scientist, Lecturer* Computer Science, Discrete Mathematics
9/1979 – 9/1981	Dept. of Applied Mathematics and Physics **Kyoto University**, Kyoto, Japan	*Visiting researcher* Network optimizations
8/1975 – 8/1985	Dept. of CS − Geometry **Eötvös Loránd University** Budapest, Hungary	*Scientist, Lecturer* Discrete/Computational geometry

Further Information

For links to my patents and publications see my personal website: https://www.hars.us/

Contact

Email: laszlo@hars.us or LaszloHars@gmail.com
Cellphone: 724-816-5073
Home office: 2078 Navajo Trail, Lafayette CO 80026. (Metro Denver).