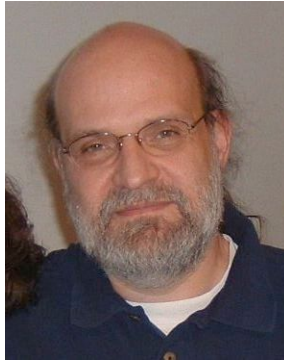


# *RESUME of Laszlo Hars*



## *Email*

- [Laszlo at Hars US](mailto:Laszlo at Hars US)
- [Laszlo period Hars at Seagate com](mailto:Laszlo period Hars at Seagate com)

## *Summary*

For 20 years I have been leading and practicing *Information Security* research and product development. I have been the chief architect of the low-level functionality of the Seagate Full Disk Encrypting (FDE) hard drives (encryption, access control, authentication, diagnostics...). I have 24+ granted patents in the field of Information Security, 46+ published patent applications (with over 20 more in the pipeline), 38 scientific publications, 4 more are under preparation.

With broad experiences in industrial research, university lecturing, product development and project management I am an expert in a wide variety of fields including **Information Security – Cryptography, DRM, Digital Watermarking, Random number generation and testing; System architecture; SW/HW development; Large Scale and Algorithmic Optimizations; Digital Signal Processing; Electronic Design and Simulations; Computational Geometry**. Besides research and lecturing I designed integrated circuits, managed large software projects and did electronic and software system design. A lot of my work led to products still in the market. I have been responsible for project schedule, risk management; selecting, training and appraisal of team members, supervised Ph.D. students.

## *Skills*

INFORMATION SECURITY RESEARCH	<b>Cryptography</b> Architect security systems; Threat models; Design and optimize <i>Elliptic Curve Cryptosystems; RSA, DES, AES</i> implementations; Implement <i>Cryptographic Toolboxes</i> ; Invent long arithmetic <i>algorithms</i> ; Design new <i>protocols, encryption modes, ciphers</i> ; Analyze security and functionality of cryptosystems <b>Tamper Resistant SW</b> improve known techniques, invent new ones <b>True Random Number Generators</b> design several new ones, improve old <b>Random Number Tests</b> design new algorithms, analyze and improve old ones
-------------------------------	--

	<p><b>Copyright Management, Media Copy Protection</b> invent, analyze and program new methods</p> <p><b>Digital Watermarking</b> new methods (for audio, image, document), apply signal processing for their test and evaluation; investigate attack scenarios</p>
ELECTRICAL ENGINEERING R & D	<p><b>Signal Quality Measurement</b> Design and build instruments for spread spectrum telecommunication systems (CDMA, GSM, DECT, NADC)</p> <p><b>Signal Generation</b> Design and build instruments for very low distortion, wide-band modulated signals</p> <p><b>Electronic Systems modeling</b> Mathematical analysis and system simulations (noise effects, distortion, phase jitter, frequency drift, quantization errors, rounding errors, ADC resolution...)</p> <p><b>Circuits Design</b> Invent new algorithms for analog and digital filters, data recorder designs, design demodulators, power supplies and other circuits</p> <p><b>Spectrum Analyzers</b> Design, construct different ones (frequency sweep, FFT)</p> <p><b>Digital Oscilloscopes</b> Design and construction; New Calibration Methods</p>
SOFTWARE DEVELOPMENT	<p><b>MATHEMATICAL RESEARCH</b> Design and program a <i>Graph</i> creating and manipulating package, equations <i>Editor</i>, program methods for <i>Planar Drawing</i> of graphs</p> <p><b>Parallelization</b> of network-, sorting- and matrix-algorithms</p> <p><b>Compiler</b> design and <b>Language</b> definition for a list manipulation language (RECS)</p> <p><b>MEDICAL SYSTEMS</b> Modeling, SW design: dosage of <i>antibiotic treatment</i>, model of <i>concentration</i> of chemicals and decomposition products in the blood; <i>Dialysis Planning</i> at severe kidney insufficiency</p> <p><b>Router</b> for VLSI design, multi-chip modules: New, improved algorithms, SW</p> <p><b>Control</b> of drawing instruments, new algorithms</p> <p><b>Utilities</b>, Electronic Musical Instruments, Simultaneous Rational Approximations</p> <p><b>Statistical</b> Estimation and Evaluation of measurement errors</p> <p><b>Combinatorial Games</b> new algorithms and programs</p>
UNIVERSITY LECTURING	<p><b>UNDERGRADUATE COURSES:</b> Geometry, Calculus, Combinatory, Combinatorial Games, Graph Theory, Computer programming</p> <p><b>GRADUATE COURSES:</b> Differential Geometry, Non-Euclidean Geometries, Discrete Geometry, Algorithmic Theory, Combinatorial Algorithms, Numerical Methods, Computational Geometry, Parallel processes, Data Structures</p>

FUNDAMENTAL RESEARCH	<p><b>Computational Geometry</b> Solve long standing open mathematical problems about optimal weighted circle placement on surfaces of constant curvature</p> <p><b>Computer Graphics</b> Develop, analyze fast second order <i>curve drawing</i> algorithms, designed data structures and algorithms for planar projections of 3D bodies</p> <p><b>Discrete Geometry</b> Investigate <i>optimal placements</i> of objects on surfaces; Study <i>Equivalence classes</i> of polyhedra by dissection</p> <p><b>Complexity of Algorithms</b> (geometric, numeric, combinatorial)</p> <p><b>Optimization</b>, improvement of numerical and combinatorial algorithms</p> <p><b>Numerical Methods</b> Invent new ones (reciprocal, inverse square root, polynomial roots, zeros of smooth functions, special functions, matrix calculations)</p> <p><b>Discrete Orthogonal Transformations</b> speed-ups, new algorithms</p> <p><b>File Allocation</b> problem solving in networks</p> <p><b>VLSI Design</b> invent optimum placement, wire routing algorithms</p>
PROFESSIONAL ACTIVITIES	<p>Panelist, National Science Foundation review of Cyber Trust (ISG) proposals (2005)</p> <p>Member of IEEE P1619 (Security In Storage) standards committee (2004 - )</p> <p>Organized, chaired the <i>Philips Information Security Workshop</i> (2001, Eindhoven)</p> <p>Coordinator of the Parallel Processing research group at the Eötvös University (1987–1989)</p> <p>Chairman of the organizing committee of the Hungarian National High-School <i>Mathematical Contest</i> (1984–1988)</p>
TOOLS MASTERED	<p>Various analog and digital <b>MEASUREMENT</b> systems</p> <p><b>SW APPLICATIONS</b>: MATLAB, Maple, Wolfram Mathematica, MS Office, VISIO...</p> <p><b>OPERATING SYSTEMS</b>: MS Windows, Virtuoso, pSOS, Unix/Linux</p> <p><b>PROGRAMMING LANGUAGES</b>: Assembler (TI DSP and x86), C/C++, Pascal, Fortran, REX, TeX, Occam, AHK, Python</p>
LANGUAGES	<p>Speak, read and write: <i>English, German, Hungarian</i></p>

## ***Degrees, Education***

**Ph.D.** in *Computational Geometry*, (Eötvös Loránd University, Budapest, 1977. Thesis: Circle Packing)

**M.Sc.** in *Mathematics and Computer Science*, (Eötvös Loránd University, Budapest 1975. Thesis: Complexity of Algorithms)

## ***Work Experience***

9/2002 –	<b>Seagate Technology</b> 389 Disc Drive Longmont, CO 80503	Principal Engineer-Scientist Manage R&D projects System design, Random Numbers,
----------	---	---

2/2000 – 8/2002	<b>Philips Research, USA</b> 345 Scarborough Rd Briarcliff Manor, NY 10510	Information Security, Cryptography Senior Scientist Lead research projects Random Numbers, Information Security, DRM
7/1998 – 2/2000	<b>Panasonic Technologies, Inc.</b> Panasonic Information and Networking Technologies Laboratory, Princeton, NJ	Senior Scientist Lead research projects Digital Watermarking, Cryptography
1/1990 – 6/1998	<b>Schlumberger Technologies</b> -> <b>Wavetek Corp.</b> Ismaning, Germany	Technology Manager, Mathematician: Mathematics and Simulations, Electronic Design, R&D Management
6/1988 – 1/1990	Institute for Operations Research <b>University Bonn, Bonn, Germany</b>	Visiting researcher VLSI design, Large Scale Optimizations
8/1985 – 9/1992	Dept. of Computer Science <b>Eötvös Loránd University</b> Budapest, Hungary	Scientist, Lecturer Computer Science, Discrete Mathematics
9/1979 – 9/1981	Dept. of Applied Mathematics and Physics <b>Kyoto University, Kyoto, Japan</b>	Visiting researcher Network optimizations
8/1975 – 8/1985	Dept. of Geometry <b>Eötvös Loránd University</b> Budapest, Hungary	Junior Scientist, Lecturer Discrete/Computational geometry

## ***Publications***

### ***Papers, Conference Presentations***

- [1] 10-Circle-Packing on the Sphere, Conference on Univ. Mathematics, Eger, 1974
- [2] In-Place Sorting (an efficient algorithm), Computer Science Conference, Szeged, 1974
- [3] Novel Phase-Shifter Circuit, Radiotechnika, 1976
- [4] Ph.D. Thesis: Weighted Circle Systems, 1977
- [5] with A. Florian, J. Molnar: On the  $\rho$ -System of Circles. Acta Math. Acad. Sci. Hung. (1977) pp. 205-221.
- [6] The Tammes Problem for  $n = 10$ . Studia Sci. Math. Hung. (1986) pp. 439-451.
- [7] Problems in Computation Theory. Notes of the Technical University of Budapest. (1987)
- [8] Circle Packing with Maximum Total Perimeter. Studia Sci. Math. Hung. 25 (1990) pp. 223-229.
- [9] On the Density of Floating Balls. Studia Sci. Math. Hung. 27 (1992) pp. 25-35.
- [10] Automatic Multi-Chip Module Wiring. Report No.90628-OR, Forschungsinstitut für Diskrete Mathematik, University Bonn.(1990) [\[pdf\]](#)

- [11] Random Search in the Traveling Salesman Problem. Report No.90629-OR, Forschungsinstitut für Diskrete Mathematik, University Bonn. (1990) [\[pdf\]](#)
- [12] Motion Control of Drawing Machines. Report, Institut für Ökonometrie und Operations Research, University Bonn. (1989) [\[pdf\]](#)
- [13] Reversible-Segment List. Report, Institut für Ökonometrie und Operations Research, University Bonn. (1989) [\[pdf\]](#)
- [14] Hybrid Heuristic for the Maximum Weighted Independent Set Problem. Report, Institut für Ökonometrie und Operations Research, University Bonn. (1989) [\[pdf\]](#)
- [15] Iterative best fit design of IIR Filters. Proceedings of the Schlumberger Signal Processing Applications Conference (1993)
- [16] Fast software division with Digital Signal Processors. Proceedings Schlumberger Signal Processing Applications Conference (1993)
- [17] Formulae and Algorithms for the GMSK Modulation, DSP World Workshop Proceedings, Toronto (1998) pp. 221-238 [\[doc\]](#) [\[pdf\]](#)
- [18] Fast Calculation of Common Mathematical Functions with Floating-Point DSPs, ICSPAT Conference Proceedings (1998), pp. 521-525.
- [19] Optimum DFT Window Design, DSP World Spring Design Conference Proceedings, Santa Clara (1999). [\[doc\]](#)
- [20] Frequency Comparator Based GFSK Demodulation, International Conference on Signal Processing and Applications and Technology, Conference Proceedings, Orlando (1999) [\[doc\]](#)
- [21] Frequency Offset Measurement of GMSK/GFSK Modulated Signals, ICSPAT, Conference Proceedings Orlando (1999) [\[doc\]](#)
- [22] Wide Range Frequency Response Compensation Using DSP, ICSPAT, Conference Proceedings, Orlando (1999) [\[doc\]](#)
- [23] Algorithmic Optimization for Floating Point DSP Mathematic Libraries, DSP World, Conference Proceedings, Orlando (1999). [\[doc\]](#)
- [24] How to Decimate with a DSP, DSP World, Conference Proceedings, Orlando (1999). [\[doc\]](#)
- [25] DSP Supported Sweeping Spectrum Analysis, ICSPAT, Conference Proceedings, Dallas (2000). [\[doc\]](#) [\[ps\]](#)
- [26] Generating Signals for Simulation and Test of Complex DSP Systems, ICSPAT, Conference Proceedings, Dallas (2000). [\[doc\]](#) [\[ps\]](#)
- [27] Frequency Response Compensation with DSP, IEEE Signal Processing Magazine, (July 2003) pp. 91-95. [\[doc\]](#), also in: Streamlining Digital Signal Processing: A Tricks of the Trade Guidebook, Richard G. Lyons (Editor), ISBN: 978-0-470-13157-2, September 2007, Wiley-IEEE Press
- [28] with M. Epstein, R. Krasinski, M. Rosner, H. Zheng: Design and Implementation of a True Random Number Generator Based on Digital Circuit Artifacts, Workshop on Cryptographic Hardware and Embedded Systems CHES 2003, Cologne, Germany (2003) [\[doc\]](#) [\[pdf\]](#)
- [29] Fast Truncated Multiplication for Cryptographic Applications, (CHES 2005), Edinburgh, [\[doc\]](#) [\[pdf\]](#) [\[ppt\]](#). Short presentation in the rump session of the 6th Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), Cambridge, MA, USA (August 2004): [\[ppt\]](#)

- [30] Applications of Fast Truncated Multiplication in Cryptography, EURASIP Journal on Embedded Systems, vol. 2007, [Article](#) ID 61721, 9 pages, 2007. doi:10.1155/2007/61721. The results were presented in CHES 2005, Edinburgh, but not printed in the proceedings because of page limitations [\[doc\]](#) [\[pdf\]](#). Short presentation in the rump session of the 6th Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), Cambridge, MA, USA (August 2004): [\[ppt\]](#). (The paper accepted for CHES'05 was resubmitted, but rejected for CHES'06 by reviewers, who did not read it. See some of their comments: [\[doc\]](#))
- [31] Long Modular Multiplication for Cryptographic Applications, Presented in the 6th Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), Cambridge, MA, USA August 2004 [\[doc\]](#) [\[pdf\]](#) [\[ppt\]](#). Cryptology ePrint archive: <http://eprint.iacr.org/2004/198/>, SpringerLink: <http://www.springerlink.com/index/M0EQ289BW2BNECL1>  
*Note:* The publisher misprinted the first version of the paper in the conference proceedings LNCS 3156. It was later corrected and re-printed.
- [32] Random Topics, Invited talk on SummerCon 2004, Pittsburgh [\[ppt\]](#)
- [33] Modular Inverse Algorithms without Multiplications, EURASIP Journal on Embedded Systems, Volume 2006 (2006), Article ID 32192: [\[url\]](#), [\[pdf\]](#) (Manuscript 2004 [\[doc\]](#) [\[pdf\]](#). Software for experiments [\[C\]](#), GMP-4.1.2 compiled into Win32 dll [\[zip\]](#).)
- [34] with R. Thibadeau: DRM Building Blocks in Secure Disk Drives, Consumer Communications & Networking Conference, CCNC'05 / CES'05, Workshop on Digital Rights Management Impact on Consumer Communications, Las Vegas (January 6, 2005) [\[ppt\]](#) [\[pdf\]](#)
- [35] with G. Petruska: Pseudorandom Recursions - Small and Fast Pseudorandom Number Generators for Embedded Applications. EURASIP Journal on Embedded Systems, vol. 2007, Article ID 98417, 13 pages, 2007. doi:10.1155/2007/98417.[\[url\]](#), [\[pdf\]](#)
- [36] Discription: Internal Hard-Disk Encryption for Secure Storage, Computer (IEEE Computer Society, ISSN 0018-9162) Vol. 40, Num 6. (June 2007), pp. 103-105. Latest version: [\[doc\]](#) [\[pdf\]](#)
- [37] Toward Standardization of Self-Encrypting Storage: Invited talk in the Security in Storage Workshop, Baltimore, September 25, 2008 [\[doc\]](#) [\[pdf\]](#) [\[ppt\]](#).
- [38] Random Number Generators in Secure Disk Drives. EURASIP Journal on Embedded Systems, vol. 2009, Article ID 598246, 10 pages, 2009. doi:10.1155/2009/598246. [\[url\]](#)

**[Issued Patents](#) (24+ on the USPTO website)**

**[Published patent applications](#) (46+ on the USPTO website)**

(~ 20 more patent applications are in the pipeline)