

# *RESUME of Laszlo Hars*

## *Summary*

For decades I have been leading and practicing *Information Security* system architecting, research and product development. I was the architect of the crypto functionality of the Seagate Self Encrypting Disk drives (SED) and Solid State Drives (encryption, access control, authentication, diagnostics...). I have 31+ granted patents, 55+ published patent applications (with over 20 more in the pipeline), 44 scientific publications, 4 more are under preparation.

With broad experiences in research, product development, project management and university lecturing 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 university lecturing I designed integrated circuits, managed large software and hardware 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 setting strategic directions of a company; for schedule and resource allocation and risk management; I defined project lines; selected, trained and appraised team members, supervised Ph.D. students and interns.

## *Skills*

INFORMATION SECURITY	<b><i>Cryptography</i></b> Architect security systems; Threat models; Design and optimize <i>Elliptic Curve Cryptosystems, RSA, DES, AES</i> implementations; <i>Cryptographic Toolboxes</i> ; Long arithmetic <i>algorithms; protocols, encryption modes, ciphers</i> ; Analyze security and functionality of cryptosystems <b><i>Tamper Resistant SW</i></b> improve known techniques, invent new ones <b><i>True Random Number Generators</i></b> design several new ones, improve old <b><i>Random Number Tests</i></b> design new tests, analyze and improve old ones <b><i>Copyright Management, Copy Protection</i></b> invent, analyze and program new methods <b><i>Digital Watermarking</i></b> new methods (for audio, image, document), apply signal processing for their test and evaluation; investigate attack scenarios
ELECTRICAL ENGINEERING R & D	<b><i>Signal Quality Measurement</i></b> Design and build instruments for spread spectrum telecommunication systems (CDMA, GSM, DECT, NADC) <b><i>Signal Generation</i></b> Design and build instruments for very low distortion, wide-band modulated signals <b><i>Electronic Systems modeling</i></b> Mathematical analysis and system simulations (noise effects, distortion, phase jitter, frequency drift, quantization errors, rounding errors, ADC resolution...) <b><i>Circuits Design</i></b> New algorithms for analog and digital filter design and

	implementation; randomness source, data recorder, demodulator, power supply and other circuit designs <b>Spectrum Analyzers</b> Designs and constructions (sweeping- and FFT-based) <b>Digital Oscilloscopes</b> Design and construction; New Calibration Methods
SOFTWARE DEVELOPMENT	<b>Mathematical SW</b> Design and program <i>Graph</i> creating and manipulating packages, equations <i>Editor</i> , new methods for <i>Planar Drawing</i> of graphs, rotate-add-XOR ciphers, Simultaneous Rational Approximations, Truncated arithmetic <b>Parallelization</b> of network-, sorting- and matrix-algorithms <b>Compiler</b> design and <b>Language</b> definition for a list manipulation language <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 <b>Router</b> New algorithms and SW for VLSI design, multi-chip modules <b>Control</b> SW and algorithms for plotters, printers <b>Utilities</b> Electronic Musical Instruments, controller for the disabled <b>Statistical</b> Estimation and Evaluation of measurement errors <b>Combinatorial Games</b> new algorithms and programs
UNIVERSITY LECTURING	<b>UNDERGRADUATE COURSES:</b> Geometry, Calculus, Combinatory, Combinatorial Games, Graph Theory, Computer programming <b>GRADUATE COURSES:</b> Differential Geometry, Non-Euclidean Geometries, Discrete Geometry, Algorithmic Theory, Combinatorial Algorithms, Numerical Methods, Computational Geometry, Parallel processes, Data Structures
FUNDAMENTAL RESEARCH	<b>Special Functions</b> Crypto applications, invertibility; Fermat numbers <b>Computational Geometry</b> Solve open mathematical problems about optimal weighted circle placement on surfaces of constant curvature <b>Computer Graphics</b> Design, analyze fast second order <i>curve drawings</i> ; data structures and algorithms for planar projections of 3D bodies <b>Discrete Geometry</b> Investigate <i>optimal placements</i> of objects on surfaces; Study <i>Equivalence classes</i> of polyhedra by dissection <b>Complexity of Algorithms</b> (geometric, numeric, combinatorial) <b>Optimization</b> , improvements of numerical and combinatorial algorithms <b>Numerical Methods</b> Reciprocal, inverse square root, polynomial roots, zeros of smooth functions, special functions, matrix calculations <b>Discrete Orthogonal Transformations</b> speed-ups, new algorithms <b>Networks</b> File allocation and traffic optimizations <b>VLSI Design</b> Placement-, wire routing algorithms

- PROFESSIONAL ACTIVITIES - Regular reviewer of scientific papers submitted for publication in international scientific journals (April 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)
  - Organized, chaired the *Philips Information Security Workshop* (2001, Eindhoven)
  - Coordinator of the Parallel Processing research group at the Eötvös Loránd University (1987–1989)
  - Chairman of the organizing committee of the Hungarian National High-School *Mathematical Contest* (1984–1988)
- TOOLS MASTERED - Various analog and digital MEASUREMENT systems
- SW Applications: MATLAB, Maple, Wolfram Mathematica, MS Office, VISIO...
  - Operating Systems: MS Windows, Virtuoso, pSOS, Unix/Linux
  - Programming Languages: Assembler (TI DSP and x86), C/C++, Pascal, Fortran, REX, TeX, Occam, AHK, Python, Julia
- LANGUAGES Speak, read and write: *English, German, Hungarian*

## *Degrees, Education*

**Post-doc scholarship:** Networked systems (Kyoto University, 1979-81)

**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*

5/2011 – present	<b>Boeing SCS ← CPU Technology, Inc.</b> 3800 Lewiston St, Ste 100 Aurora, CO 80011	Chief Cryptologic Architect System design, Random Numbers, Information Security, Cryptography
9/2002 – 5/2011	<b>Seagate Technology</b> 389 Disc Drive Longmont, CO 80503	Principal Engineer-Scientist Manage R&D projects System design, Random Numbers, Information Security, Cryptography
2/2000 – 8/2002	<b>Philips Research, USA</b> 345 Scarborough Rd Briarcliff Manor, NY 10510	Senior Scientist Lead research projects Random Numbers, Information Security,

7/1998 – 2/2000	<b>Panasonic Technologies, Inc.</b> Panasonic Information and Networking Technologies Laboratory, Princeton, NJ	DRM 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</b> , Bonn, Germany	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</b> , Kyoto, Japan	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. Presented in **CHES 2005**, Edinburgh, but not printed in the proceedings. [\[doc\]](#) [\[pdf\]](#). 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 rejected for CHES'06: [\[doc\]](#))

- [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 Report 2004/198 [\[url\]](#), SpringerLink: [\[url\]](#) (**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] Discryption: 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. [\[url\]](#)
- [39] with others: IEEE P1619 SISWG, Standard for Narrow-Block Encryption [\[url\]](#)
- [40] with others: IEEE P1619 SISWG, Standard for Authenticated Encryption [\[url\]](#)
- [41] with others: IEEE P1619 SISWG, Standard for Wide-Block Encryption [\[url\]](#)
- [42] with others: IEEE P1619 SISWG, Standard for Key Management [\[url\]](#)
- [43] with G. Petruska: Pseudorandom Recursions II. [\[doc\]](#) [\[pdf\]](#) EURASIP Journal on Embedded Systems 2012, 2012:1 doi:10.1186/1687-3963-2012-1 [\[url\]](#).
- [44] Random Number Generation Based on Oscillatory Metastability in Ring Circuits. Cryptology ePrint Archive: Report 2011/637 [\[url\]](#) [\[doc\]](#) [\[pdf\]](#)

[Issued Patents \(31+ on the USPTO website\)](#)

[Published patent applications \(55+ on the USPTO website\)](#)

(More publications and patent applications are in preparation.)