

RESUME

Laszlo Hars, PhD

Webpage: www.hars.us, Email: laszlo@hars.us

SUMMARY

For 18 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 21 granted patents in the field of Information Security, 41 published patent applications (with over 22 more in the pipeline), 37 scientific publications, 4 more are submitted this year.

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 **Cryptography** Architect security systems; Threat models; Design and optimize *Elliptic Curve Cryptosystems; RSA, DES, AES* implementations; Implement *Cryptographic Toolboxes*; Invent long arithmetic *algorithms*; Design new *protocols, encryption modes, ciphers*; Analyze security and functionality of cryptosystems
Tamper Resistant SW improve known techniques, invent new ones
True Random Number Generators design several new ones, improve old
Random Number Tests design new algorithms, analyze and improve old ones
Copyright Management, Media Copy Protection invent, analyze and program new methods
Digital Watermarking new methods (for audio, image, document), apply signal processing for their test and evaluation; investigate attack scenarios

ELECTRICAL ENGINEERING R & D **Signal Quality Measurement** Design and build instruments for spread spectrum telecommunication systems (CDMA, GSM, DECT, NADC)
Signal Generation Design and build instruments for very low distortion, wide-band modulated signals
Electronic Systems modeling Mathematical analysis and system simulations (noise effects, distortion, phase jitter, frequency drift, quantization errors, rounding errors, ADC resolution...)

	<p>Circuits Design Invent new algorithms for analog and digital filters, data recorder designs, design demodulators, power supplies and other circuits</p> <p>Spectrum Analyzers Design, construct different ones (frequency sweep, FFT)</p> <p>Digital Oscilloscopes Design and construction; New Calibration Methods</p>
SOFTWARE DEVELOPMENT	<p>MATHEMATICAL RESEARCH 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>Parallelization of network-, sorting- and matrix-algorithms</p> <p>Compiler design and Language definition for a list manipulation language (RECS)</p> <p>MEDICAL SYSTEMS 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>Router for VLSI design, multi-chip modules: New, improved algorithms, SW</p> <p>Control of drawing instruments, new algorithms</p> <p>Utilities, Electronic Musical Instruments, Simultaneous Rational Approximations</p> <p>Statistical Estimation and Evaluation of measurement errors</p> <p>Combinatorial Games new algorithms and programs</p>
UNIVERSITY LECTURING	<p>UNDERGRADUATE COURSES: Geometry, Calculus, Combinatory, Combinatorial Games, Graph Theory, Computer programming</p> <p>GRADUATE COURSES: Differential Geometry, Non-Euclidean Geometries, Discrete Geometry, Algorithmic Theory, Combinatorial Algorithms, Numerical Methods, Computational Geometry, Parallel processes, Data Structures</p>
FUNDAMENTAL RESEARCH	<p>Computational Geometry Solve long standing open mathematical problems about optimal weighted circle placement on surfaces of constant curvature</p> <p>Computer Graphics Develop, analyze fast second order <i>curve drawing</i> algorithms, designed data structures and algorithms for planar projections of 3D bodies</p> <p>Discrete Geometry Investigate <i>optimal placements</i> of objects on surfaces; Study <i>Equivalence classes</i> of polyhedra by dissection</p> <p>Complexity of Algorithms (geometric, numeric, combinatorial)</p> <p>Optimization, improvement of numerical and combinatorial algorithms</p> <p>Numerical Methods Invent new ones (reciprocal, inverse square root, polynomial roots, zeros of smooth functions, special functions, matrix calculations)</p> <p>Discrete Orthogonal Transformations speed-ups, new algorithms</p> <p>File Allocation problem solving in networks</p> <p>VLSI Design 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 Various analog and digital *MEASUREMENT* systems
MASTERED **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

LANGUAGES Speak, read and write: *English, German, Hungarian*

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 –	Seagate Research 1251 Waterfront Place Pittsburgh, PA 15222	Principal Engineer-Scientist Manage R&D projects System design, Random Numbers, Information Security, Cryptography
2/2000 – 8/2002	Philips Research, USA 345 Scarborough Rd Briarcliff Manor, NY 10510	Senior Scientist Lead research projects: Random Numbers, Information Security, DRM
7/1998 – 2/2000	Panasonic Technologies, Inc. Panasonic Information and Networking Technologies Laboratory, Princeton, NJ	Senior Scientist Lead research projects Digital Watermarking, Cryptography
1/1990 – 6/1998	Schlumberger Technologies / Wavetek Corp. Ismaning, Germany	Technology Manager, Mathematician: Mathematics and Simulations, 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 Geometry Eötvös Loránd University Budapest, Hungary	Junior Scientist, Lecturer Discrete/Computational geometry

PUBLICATIONS

- [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 ρ -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)
- [11] Random Search in the Traveling Salesman Problem. Report No.90629-OR, Forschungsinstitut für Diskrete Mathematik, University Bonn. (1990)
- [12] Motion Control of Drawing Machines. Report, Institut für Ökonometrie und Operations Research, University Bonn. (1989)
- [13] Reversible-Segment List. Report, Institut für Ökonometrie und Operations Research, University Bonn. (1989)
- [14] Hybrid Heuristic for the Maximum Weighted Independent Set Problem. Report, Institut für Ökonometrie und Operations Research, University Bonn. (1989)
- [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.
- [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).
- [20] Frequency Comparator Based GFSK Demodulation, International Conference on Signal Processing and Applications and Technology, Conference Proceedings, Orlando (1999)
- [21] Frequency Offset Measurement of GMSK/GFSK Modulated Signals, ICSPAT, Conference Proceedings Orlando (1999)
- [22] Wide Range Frequency Response Compensation Using DSP, ICSPAT, Conference Proceedings, Orlando (1999)
- [23] Algorithmic Optimization for Floating Point DSP Mathematic Libraries, DSP World, Conference Proceedings, Orlando (1999).
- [24] How to Decimate with a DSP, DSP World, Conference Proceedings, Orlando (1999).
- [25] DSP Supported Sweeping Spectrum Analysis, ICSPAT, Conference Proceedings, Dallas (2000).
- [26] Generating Signals for Simulation and Test of Complex DSP Systems, ICSPAT, Conference Proceedings, Dallas (2000).
- [27] Frequency Response Compensation with DSP, IEEE Signal Processing Magazine, (July 2003) pp. 91-95. 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)
- [29] Fast Truncated Multiplication for Cryptographic Applications, (CHES 2005), Edinburgh. Short form: Rump session of the 6th Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), Cambridge, MA, USA (August 2004)
- [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. Also presented in CHES 2005, Edinburgh. Short presentation in the rump session of the 6th Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), Cambridge, MA, USA (August 2004)

- [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. Cryptology ePrint archive: <http://eprint.iacr.org/2004/198/>, SpringerLink: <http://www.springerlink.com/index/M0EQ289BW2BNECL1>.
- [32] Random Topics, Invited talk on SummerCon 2004, Pittsburgh
- [33] Modular Inverse Algorithms without Multiplications, EURASIP Journal on Embedded Systems, Volume 2006 (2006), Article ID 32192. (Manuscript 2004)
- [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)
- [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.
- [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.
- [37] Toward Standardization of Self-Encrypting Storage: Invited talk in the Security in Storage Workshop, Baltimore, September 25, 2008.

Patents

PAT. NO.	Title
1	7,363,564 Method and apparatus for securing communications ports in an electronic device
2	7,360,057 Encryption of data in a range of logical block addresses
3	7,356,552 VLSI implementation of a random number generator using a plurality of simple flip-flops
4	7,356,551 Method and apparatus of retaining maximum speed of flip-flop metastability based random number generators
5	7,325,021 VLSI implementation of metastability-based random number generator using delay ladders
6	7,315,874 Electronic circuit for random number generation
7	7,302,575 Apparatus for and method of preventing illicit copying of digital content
8	7,302,458 Method and apparatus for choosing a combination of logic for generating random numbers using a difference signal
9	7,295,674 On-line randomness test for detecting irregular pattern
10	7,213,004 Apparatus and methods for attacking a screening algorithm based on partitioning of content
11	7,124,155 Latching electronic circuit for random number generation
12	7,047,262 Entropy estimation and decimation for improving the randomness of true random number generation
13	7,031,991 Hadamard-transform on-line randomness test
14	6,993,543 Gap histogram on-line randomness test
15	6,947,960 Randomness test utilizing auto-correlation
16	6,925,342 System and method for protecting digital media
17	6,889,236 Gap average on-line randomness test
18	6,771,104 Switching electronic circuit for random number generation
19	6,763,366 Method for calculating arithmetic inverse over finite fields for use in cryptography
20	6,745,220 Efficient exponentiation method and apparatus
21	6,675,113 Monobit-run frequency on-line randomness test

Published patent applications (some 22 more patent applications are in the pipeline)

PUB.APP.NO.	Title
1	20080201536 Near instantaneous backup and restore of disc partitions
2	20080155262 System and method for tamper evident certification
3	20080114981 Method and apparatus for authenticated data storage
4	20080072071 Hard disc streaming cryptographic operations with embedded authentication
5	20070033454 Method and apparatus for securing communications ports in an electronic device
6	20060230460 Hierarchical scheme for secure multimedia distribution
7	20060218647 Data transcription in a data storage device
8	20060218412 Data encryption in a data storage device
9	20060200682 Apparatus and method for protecting diagnostic ports of secure devices
10	20060198515 Secure disc drive electronics implementation
11	20060133607 Apparatus and method for generating a secret key
12	20060064489 Method for limiting the number of network devices in a communication network
13	20060005046 Secure firmware update procedure for programmable security devices
14	20050286351 Stable disc controller ID from unstable comparator outputs
15	20050210257 System and method for protecting digital media
16	20050004961 Method and apparatus of retaining maximum speed of flip-flop metastability based random number generators
17	20050004960 Electronic circuit for random number generation
18	20050004959 VLSI implementation of metastability-based random number generator using delay ladders
19	20040267846 Method and apparatus for choosing a combination of logic for generating random numbers using a difference signal
20	20040267845 VLSI implementation of a random number generator using a plurality of simple flip-flops
21	20040049525 Feedback random number generation method and system
22	20040039762 Entropy estimation and decimation for improving the randomness of true random number generation
23	20040019617 Latching electronic circuit for random number generation
24	20040017235 SWITCHING ELECTRONIC CIRCUIT FOR RANDOM NUMBER GENERATION
25	20030200489 Secure method of and system for rewarding customers
26	20030200239 Gap histogram on-line randomness test
27	20030200238 Hadamard-transform on-line randomness test
28	20030200140 Secure method of and system for rewarding customer
29	20030187890 Gap average on-line randomness test
30	20030187889 Functional gap average on-line randomness test
31	20030187598 Monobit-run frequency on-line randomness test
32	20030158876 On-line randomness test through overlapping word counts
33	20030158875 Randomness test utilizing auto-correlation
34	20030156713 On-line randomness test for detecting irregular pattern
35	20030088774 Apparatus for and method of preventing illicit copying of digital content
36	20030088773 Method of and apparatus for preventing illicit copying of digital content
37	20020174155 Method for calculating arithmetic inverse over finite fields for use in cryptography
38	20020152172 Apparatus and methods for attacking a screening algorithm based on partitioning of content
39	20020076048 System and method for inserting disruptions into merged digital recordings
40	20020073317 System and method for protecting digital media
41	20020068987 System and method for protecting digital media