RESUME of Laszlo Hars, PhD

Chief Crypto Architect of Boeing SCS

Boeing Technical Fellow

Summary

For decades I have been leading and practicing research and development in *Information Security* and *Security System Architecture*. 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 53+ granted patents, 110+ patent applications, and 47 scientific publications, with more under preparation.

With broad experiences in research, product development, project management and systems architecture, I am an expert in a wide variety of fields including Information Security – *Information Assurance, Cryptography, Anti Tamper (AT), DRM, Digital Watermarking, Security architecture; SW/HW development; Large Scale and Algorithmic Optimizations; Digital Signal Processing; Electronic Design and Simulations; Mathematics,* and *Computer Science*. Besides R&D and university lecturing I designed integrated circuits, managed large software and hardware projects and did electronic and software systems design. A lot of my work led to products currently in the market.

I have been responsible for setting strategic directions of companies; for schedule and resource allocation and risk management; I defined project lines; selected, trained and appraised team members, supervised Ph.D. students and interns.

Recent Projects

- Memory encryption for secure processors (internal, external)
- Protection of data in storage devices
- Boot counters in ASICs
- Random number generators, Electronic entropy sources, Randomness tests
- Physical Unclonable Functions, Manufacturing process variations
- Masking schemes for ciphers
- Quantum computing resistant cryptography
- Self-tests for security electronics
- Boot image authentication
- Lightweight cryptography
- Bit-mixers and their applications in Information Security

Skills

INFORMATION SECURITY	***Cryptography*** Security systems architecture; Threat models; Design, implementations and optimization of *Cryptosystems*; *Cryptographic Toolboxes*; Long arithmetic *algorithms*; Communication *protocols*, Encryption *modes*, novel *ciphers*; Security and functionality analyzes of cryptosystems ***Anti-Tamper (AT)*** analyzed, devised physical attacks, developed countermeasures ***Tamper Resistant SW*** improved known techniques, invent new ones ***Random Number Generators, PUFs*** designed several new ones, improve old ***Random Number Tests*** designed new tests, analyzed and improved old ones ***Copyright Management***, ***Copy Protection*** invented, analyzed and programmed new methods ***Digital Watermarking*** new methods (for audio, image, document), applied signal processing for test and evaluation; investigated attack scenarios
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, quantization errors, rounding errors, ADC resolution…) ***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	***Mathematical SW*** Design and program *Graph* creating and manipulating packages, equations *Editor*, new methods for *Planar Drawing* of graphs, rotate-add-XOR ciphers, 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 plotters, printers ***Utilities*** Electronic Musical Instruments, controllers for the disabled ***Statistical*** Estimation and Evaluation of measurement errors ***Combinatorial Games*** new algorithms and programs

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*** Solved open mathematical problems about optimal weighted circle placement on surfaces of constant curvature ***Computer Graphics*** Designed, analyzed fast second order *curve drawings;* data structures and algorithms for planar projections of 3D bodies ***Discrete Geometry*** Investigated *optimal placements* of objects on surfaces; Study *Equivalence classes* of polyhedra by dissection ***Complexity of Algorithms*** (geometric, numeric, combinatorial) ***Optimization***, improvements of numerical and combinatorial algorithms ***Numerical Methods*** Reciprocal, inverse square root, polynomial roots, zeros of 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

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)
- **Diploma** in Economics ML University, Budapest 1978.

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 (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)
- Organizer, chairman of the Philips Information Security Workshop (2001, Eindhoven)
- Coordinator of the Parallel Processing research group, 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

Work Experiences

5/2011 – present	**Boeing SCS <– CPU Technology, Inc.** 5753 W. Las Positas Blvd. Pleasanton CA 94588-4084	*Chief Crypto Architect* System design, RNGs, PUFs, InfoSec Security, AT, Cryptography, Crypto 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 Scientist* Lead research projects Random Numbers, InfoSec, 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	*Chief Technologist* 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	*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 ***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) [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]

[45] Cryptographic and Algorithmic Protection of External Memory of Secure Microprocessors, 2015 National Anti-Tamper Review, 14-16 April 2015 Johns Hopkins University.

[46] Hardware Bit-Mixers. Cryptology ePrint Archive: Report 2017/084: https://eprint.iacr.org/2017/084

[47] Information Security Applications of Bit-Mixers. Cryptology ePrint Archive: Report 2017/085: https://eprint.iacr.org/2017/085

Patents

Issued Patents **(2016: 53+ *on the USPTO website*)**

Published patent applications **(2016: 72+ *on the USPTO website*)**

(40+ more inventions have been disclosed)