Research Archive

Prof. Wael Adi

IDA: Institute for Computer and Communication Networks

Electrical Engineering Department

Technical University of Braunschweig

Research Activities 1975-1985:

- Error correction technology
- Relational data base machines
- High Speed VLSI for fault tolerant Computer systems
- High speed hardwired relational join operation
- VLSI architectures for burst error correcting codes for disc memory

Research Activities 1996-2002:

"Reliability & Security Research Group" at the institute for computer engineering and communication networks TU Braunschweig:

1) New architectures for mobile communication channel coding
2) Security mechanisms for large communication networks
3) VLSI architectures for coding and cryptography
4) Mobile security and mobile assisted payment systems
5) Security and cash equivalent e-money
6) High speed VLSI architectures for security applications

The group has completed the following research projects:

Funded research 1997-2002:

1. ISATEC: Parallel Array Processing for Elliptic Curve Cryptosystems over GF(2^m)
2. MAGENTA Encryption VLSI Engine (German telecom research center, Darmsradt)
3. UMTS/ 3GPP, Mobile Security and Coding with BOSCH Telecom and SIEMENS
4. Internet Security with DFAM e.V. (German res. community for applied microelectronics)
5. VLSI architectures for communication protocols Sci-worx/SIEMENS
6. VLSI architecture for smart card security functions (AES, KASUMI ciphers) Sci-worx/SIEMENS

Research partner: SIEMENS AG, BOSCH Telecom, DFAM e.v, ISATEC, German Telecom Research Center, Sci-Worx/Siemens (VLSI), Volkswagen AG

Research Activities 2002 -2005:

1. E-Commerce and Mobile commerce (Comtrust UAE Telecom)
2. Cryptographic protocols and mechanisms for E-Money (FairCash Project application, FP6 EC research application together with TU Kiel, Tuebingen, New Castle UK.
3. Cryptographic mechanisms for Intellectual Property Right protection in VLSI/FPGA design environment (3 Patents and 4 papers in progress)
4. Security mechanisms in Robot environment. Secured unique Robot genetic codes (initial cooperation, Samsung)
5. Image security with reduced complexity (Basic research)
6. Ultra high-speed I-CRT VLSI Architectures (one patent and industrial cooperation in progress Bosch Electronics Stuttgart)
7. E-Voting
8. IPR protection for VLSI designs in FPGA environment

Former Research History 1986–1996:

From 1986 to 1996, Dr. Adi chaired the **Department of Applied Research** at the **Institute for Applied Microelectronics** Braunschweig/Germany. The following includes a summary of his 10 years activities:

Applied research:

1985-1986 Research with. Siemens (Munich/Germany), Conceptions and VLSI-Architectures for error correcting codes, ca. 8000 Gates Gate Array.

1992-1993 Project management for the design of a multiprocessor ASICs for a Communication protocol (PROFIBUS-Master, ca.70 K Gate), EC Program: JESSI Working Group

1993-1994 Technical conceptions and building a JESSI Working group for a Universal Crypto-VLSI (Volume ca. 1.3 Million DM)

1992-1994 VLSI architectures of hash-based ultra-fast fuzzy scoring mechanisms for natural language search. MIT Inc. USA

1991-1994 Error correction coding for periodically disturbed channels, German Research Council (DFG)

1990-1994 Hardware architectures and encoding/decoding mechanisms for ultra fast processing (IAM)

1990-1996 VLSI architectures for the crypto-systems: DES, IDEA, RSA, Stream-Ciphers, Smart-Card-Systems (IAM)

Industrial projects in microelectronics:

Applied research for microelectronics industry:

1. Crypto-Mapping function for identification" Volkswagen AG, July 1988.
2. ASIC for error correcting code for disk memory 1990-1991, SIEMENS AG.
3. DSP-Software and VLSI for GSM error correcting Fire-Code 1990-1991, Robert Bosch GmbH, Berlin.
4. VLSI-Code-design for RS-like error correction. Integration ca. 13.000 Gates 1988-1990. SIEMENS AG.
5. "Unidirectional Error Correcting Codes for EEPROM Applications," 1988, ALVO/Philips.
6. "Self-synchronizing PN-Sequence Generator for Measuring Channel Errors," 1988, VALVO/Philips.
7. High-Speed VLSI (13ns) 2-Byte Error Correction (Reed Solomon Code), 52.000 Gates," 1994/95 SIEMENS
8. "Single Error Correcting Code for Very High-Speed System with Nibble-Detection," 1994, SIEMENS AG.
9. VLSI Architecture for Ultra-Fast 1-Nibble Error Correction (1995-96). SIEMENS AG.

Designed and/or lead the design and research for more than 50 VLSI/ASIC Chips, the following is a selected extract:

1. VLSI for Viterbi-Convolutional Code Encoder-Decoder in VHDL (1993)
2. Ultra high speed CRT based error location VLSI architecture
3. 8051 Processor VHDL Model, with FPGA Prototyping 1992-1994.
4. PIC 16 Processor VHDL Model, 1994.
5. Automatic generation of nxm Bit Multiplier and VHDL Synthesis 1995.
6. Asynchronous VLSI unit distance code counting with hazard free comparison 1993
7. VLSI Architecture for fast Burst Error Correcting GSM Fire Code, 1992.
8. VLSI Architecture for 2 Error-Correcting BCH Code (1986)
9. VLSI Engine for Fuzzy Linguistic Score Evaluation (1989)
10. Track error correcting code for Tape-Memory in ANSI-C and VLSI (1987)
11. VLSI Architecture for High Speed error location decoding (1991)
12. VLSI for Ultra High-Speed Hash-based Association Engine (1990)
13. ASICs for industrial memory programmable control (SPS), 1986-1989
14. Stream-Cipher with PCI-Interface in VHDL and FPGA , (1995-1997)
15. High Speed VLSI Reed-Solomon Error Correcting Chip (1988)
16. VLSI for DES Cipher (1995)
17. High-Sped IDEA Ciphering machine in VLSI (1993)
18. ASIC for PROFIBUS-MASTER Communication-protocol, (80 K Gates) 1991-1994.

Miscellaneous:

19. Generating CCIR Radio Paging code No 1 (in ANSI-C).
20. Prime Number Generation (in ANSI-C).
21. Exponentiation and Arithmetic over GF(2^{1024}) (in ANSI-C).
22. Exponentiation and Arithmetic over GF(p), p⇔ 1024 Bits (in ANSI-C).
23. DES Ciphering machine in VLSI and in ANSI-C
24. High Current surge generator (up to 3000 A, 1000 A/µs), 1990.
25. SMART CARD Interface with 8051 controller, 1992.

Note: Due to the classified nature of the industrial research projects, no publications were permitted from 1986 to 1996.