

Mahadevan Gomathisankaran

Curriculum Vitae

Contacts

University of North Texas
Computer Science and Engineering, F227
3940 N. Elm
Denton, TX 76207

mgomathi@unt.edu
<http://www.cse.unt.edu/~mgomathi>
(+1) 940.565.4864

Research Interests

Secure Systems Architecture
Cryptography
Low power VLSI design

Education

Ph.D., Computer Engineering, May 2006

Iowa State University, Ames, IA.

Thesis: *Secure execution environments through reconfigurable lightweight cryptographic components.*

Adviser: Dr. Akhilesh Tyagi

Committee: Dr. Soma Chaudhuri, Dr. Thomas Daniels, Dr. Randall Geiger, and Dr. Zhao Zhang

GPA: 3.96/4.0

Bachelors, Electronics and Communication Engineering, May 1998

Regional Engineering College, Trichy, India.

GPA: 85.6%, *First Class with Distinction.*

Honors

IBM Ph.D. Fellowship

Awarded for two academic years (2004 & 2005)

Acceptance rate: 50 out of worldwide applicants

Premium for Academic Excellence Award (PACE)

Awarded by Iowa State University for the year 2002

Acceptance percentage: 10%

Publications

Journal Articles

M. Gomathisankaran and A. Tyagi. **Relating Boolean Gate Truth-tables to One-way Functions.** *Integrated Computer Aided Engineering*, 16(2): 141-150, 2009.

M. Gomathisankaran and A. Tyagi. **Architecture Support for 3D Obfuscation.** *IEEE Trans. Computers*, 55(5):497-507, 2006.

M. Gomathisankaran and A. Tyagi. **WARM SRAM: A novel scheme to reduce static energy leakage in SRAM Arrays.** *J. Low Power Electronics*, 2(3):388-400, 2006.

Conference Papers

M. Gomathisankaran and R. B. Lee. **Tantra: A fast PRNG algorithm and its implementation.** To appear in the proceedings of *International Conference on Security and Management (SAM'09)*, 2009.

M. Gomathisankaran, R. B. Lee. **Maya: A Novel Block Encryption Function.** To appear in pre-proceedings of *International Workshop on Coding and Cryptography*, 2009.

M. Gomathisankaran, K. Keung, and A. Tyagi. **REBEL: Reconfigurable Block Encryption Logic.** In *International Conference on Security and Cryptography (SECRYPT)*, 26-29 July 2008, Porto, Portugal.

M. Gomathisankaran and A. Tyagi. **Relating Boolean Gate Truth-tables to One-way Functions.** In *IEEE International Conference on Electro/Information Technology (EIT)*, May 2008, Ames, IA.

M. Gomathisankaran and A. Tyagi. **TIVA: Trusted Integrity Verification Architecture.** In *First International Conference on DRM Technologies, Issues, Challenges and Systems (DRMTICS)*, Nov 2005, Sydney, Australia.

M. Gomathisankaran and A. Tyagi. **A 3D Obfuscation Architecture.** In *High Performance Embedded Architectures and Compilers (HiPEAC)*, Oct 2005, Barcelona, Spain.

M. Gomathisankaran and A. Tyagi. **WARM SRAM: A novel scheme to reduce static leakage energy in SRAM Arrays.** In *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Feb 2004.

Technical Reports

M. Gomathisankaran and A. Tyagi. **How to hide secrets from OS: Architecture Level Support for Dynamic Address Trace Obfuscation.** *Iowa State University*, Aug 2004.

M. Gomathisankaran and A. Somani. **Efficient Energy Saving Scheme for On-chip Caches.** *Iowa state University*, Nov 2002.

Under Submission

J. Dwoskin, M. Gomathisankaran and R. Lee. **Framework for Design Validation of Security Architectures.**

Patents

A. Tyagi and M. Gomathisankaran. **REBEL: Reconfigurable Block Encryption Logic.** *Iowa State University*, patent pending, ISURF #3404.

Research Experience

Post Doctoral Research

Secure systems solution involve both hardware and software components. Conventional way of testing these solutions is to reason the strengths and weaknesses of the architecture and test these components independently. The correctness of such an approach is entirely dependent on the designer of those components. We are investigating a novel testing framework that allows testing of both hardware and software components together in a realistic execution environment. We are designing and developing such a framework using virtualization technology.

Graduate Research

Reconfigurable Block Encryption Logic:

Conventional block ciphers (DES,AES) derive their security from an embedded secret, more commonly referred to as a key. The secret, however, is combined with the state in a limited way, as an xor, during a round. The xor based mixing of the cipher state and the secret leads to some vulnerabilities based on linear and differential cryptanalysis. The complexity of extracting the secret or its properties is proportional to the non-linearity, among many other attributes, of the round functions. We proposed a simple yet novel approach wherein the round functions themselves become the secret, while the function schema is a publicly published algorithm. The intuition is to use reconfigurable gates as round functions and define their configurations as the secret (or key). Hence the complexity of such a cryptographic function is derived from the fact that almost all of the round processing is driven by the secret (truth tables).

Efficient solution to memory integrity verification problem:

Embedded devices are omnipresent and pervade all facets of human life. Their sheer numbers and wide presence make them amenable to tampering. A tampered sensor could misrepresent its environment or a tampered PDA could relay the private data of the user to a third party. Hence verification of these devices is a relevant problem. However, such verification needs to be extremely efficient and mostly automated given the sheer numbers of these devices. Moreover, the verification architecture will not be practical if it compromises the IP of the software running on these devices. We proposed a novel hardware architecture TIVA and a schema for such a verification mechanism which satisfies all the requirements of a verification system without compromising the IP of the system being verified.

Architecture support for 3D Obfuscation:

Software obfuscation is a key technology in IP-protection. However, software only solutions often do not have robustness of crypto methods. Complete control flow obfuscation methods such as Cloakware have the limitation that they cannot hide the correct control flow information from the prying eyes of the OS/end user. An additional weakness in these schemes is that observation of repeated dynamic execution often gives away the obfuscation secrets. We proposed a minimal architecture, *Arc3D*, to support efficient obfuscation of both static binary file system image and dynamic execution traces. This obfuscation covers three aspects: address sequences, contents, and second-order address sequences.

Leakage energy reduction in SRAM Arrays:

Static subthreshold leakage has emerged as one of the major impediments in CMOS scaling. Microprocessors attain significant performance improvement by increasing the size and associativity of on-chip caches. Both *dynamic* switching energy, and *static* subthreshold leakage current induced energy of on-chip caches are already significant factors in over-all power consumption of the processors. The static leakage energy would overwhelm the dynamic energy for these caches as the static energy grows exponentially with reduction in feature size. We presented a SRAM cell design in dep-warmup CMOS and its block level implementation. The detailed SPICE simulations estimate the static leakage energy savings for L1 caches at more than 90% without any affect on the performance.

Teaching Experience

Lab Coordinator

Teaching Assistant for two semesters for "Introduction to Micro-controllers" (CPRE211) course at Iowa State University. My responsibilities included coordinating the labs, setting up the exercises, and grading. I enjoyed the experience of interacting with students during these lab sessions. This was a real motivating factor for my choice of academic career.

Teaching Assistant

Assisted Dr. Akhilesh Tyagi with his "Advanced Computer Architecture" (CPRE681) graduate level course. I prepared and delivered lectures related to the recent research works in the area of *Secure Computer Architectures*.

Industry Experience

Jul 06 – Nov 07 *Research Scientist*, Intel Systems Research Center, Bangalore

Involved in the research of providing a Trusted Place to Stand in Many Core Platforms. Virtualization is a key technology that will enable the use of many core platforms. Trust to the platform is projected from the Trusted Platform Module (TPM). The key research issue that I worked on is to project this trust on to multiple Virtual Machines.

May05 – Aug 05 *Intern*, IBM TJ Watson Research Center, Hawthorne, NY

Part of Secure Systems group. Worked on IBM PowerPC simulator to implement the proposed secure architecture *Arc3D*.

Jan 04 – Jul 04 *Intern*, Intel, Chandler, AZ

Designed, developed and documented test cases for XScale and NPE in IXP4XX. Designed and developed automated testing module in XScale to load and test various test cases of NPE's. Awarded for *excellent performance* during Internship.

Aug 00 – Jul 02 *Software Design Engineer*, Texas Instruments India, Bangalore

Ported EPOC device driver for ARM processor in OMAP (TI's dual processor wireless architecture). Worked in Real Time Data Exchange (RTDX) for TMS320C28x, which uses the in-circuit-emulator on the DSP to transfer data between host(PC) and target(DSP). Experienced in TI's emulation architecture and real time emulation technology.

Jul 98 – Jul 00 *Software Engineer*, Philips Software Center, Bangalore

Designed and developed various features like Picture in Picture (PIP), Multi PIP, Freeze, PhotoFinish, Closed Caption Decoder, and Replay on 8051XA (8-bit microcontroller) using KOALA software architecture.

Awards

2004 Awarded for excellent performance during internship at Intel

2000 Awarded merit bonus for the significant contribution to the DSP Bridge project at Texas Instruments India

1998 – 1999 Rated excellent in the two yearly appraisals at Philips Software Center

1994 – 1998 Recipient of merit-cum-means scholarship for four academic years at Regional Engineering College Trichy

References

Upon Request

Updated On: 08/27/09