MOSTAFA TAHA

Electrical Engineering Department,
Assiut University, Assiut, Egypt.
Phone: +201009488422
Email: mtaha@aun.edu.eg

I am currently an Assistant Professor at the Electrical Engineering Department of Assiut University, Egypt, working in the area of hardware security and implementation attacks. I got my PhD degree from the Secure Embedded Systems lab at Virginia Tech, advised by Dr. Patrick Schaumont and worked as a postdoctoral fellow at the Vernam Research Group of Worcester Polytechnic Institute. My research focus on the side-channel analysis of different cryptographic schemes.

EDUCATION

- *Doctor of Philosophy*, Computer Engineering
  Virginia Tech, Blacksburg, VA GPA 3.88 May 2014
  Dissertation: Advances in the Side-Channel Analysis of Symmetric Cryptography
- *Master of Science*, Electrical Engineering
  Assiut University, Egypt GPA 3.62 December 2008
  Thesis: Broadcasting protocols in Vehicular Ad-Hoc Networks
- *Bachelor of Science*, Electrical Engineering
  Assiut University, Egypt GPA 3.86 May 2004

RESEARCH EXPERIENCE

My research focuses on mounting/protecting against Implementation Attacks, a field of Cryptographic Engineering. During my PhD research, I participated in the following projects:

- *Attacking Block-Ciphers:*
  -*Power Attacks:* We proposed a novel method for analyzing high parallel implementations. The power consumption of AES on SASEBO-GII was exploited, and the results were presented at ICCD'12.
  -*Fault Attacks:* Together with N. Ghalaty, we proposed a new concept for mounting Differential Fault Attacks. The results of this project are currently under review.
- *Protecting Block-Ciphers:*
  -*Hiding:* Together with S. Mane, we designed a set of balanced custom instructions to prevent the electromagnetic leakage of AES on Nios-II processor. The results were presented at FPL'12.
  -*Masking:* Together with H. Eldib, we developed a metric for quantifying the masking strength of software implementation right from the source code. The results were accepted at DAC'14.
  -*Leakage Resiliency:* We proposed a framework for practical leakage resiliency, with two solutions for AES. One solution used NLFSRs, while the other used round-reduced version of AES. Preliminary results were presented at DIAC'13, while advanced results are currently under review.
- *Attacking Hashing Functions:*
  We exploited the power consumption of the new SHA-3 hashing standard. We targeted both Microblaze processor and a 0.13μm ASIC chip. Results of this project were presented at HOST'13, and IWSEC'13.
- *Protecting Hashing Functions:*
  We developed a lightweight secure core for all the keyed and unkeyed applications of SHA-3. Our solution has no area overhead, very low performance overhead, and can be tuned or turned-off. Results of this project were accepted at HOST'14.

MSc Research: During the MSc degree, we proposed a reliable broadcasting protocol for life-safety messages in Vehicular Ad-Hoc Networks (VANETs). Results of this research were presented in ISSPIT'07 and VTC'08.

PUBLICATIONS

1. **M. Taha**, P. Schaumont 'Key Updating for Leakage Resiliency With Application to AES Modes of Operation,' IEEE Transactions on Information Forensics and Security, vol.10, no.3, pp.519,528, March 2015.
2. N. Ghalaty, B. Yuce, **M. Taha**, P. Schaumont, 'Differential Fault Intensity Analysis,' 11th Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2014), Busan, Korea, September 2014.
3. **M. Taha**, P. Schaumont 'Side-Channel Countermeasure for SHA-3 at Almost-Zero Area Overhead,' IEEE Symposium on Hardware Oriented Security and Trust (HOST-2014), Arlington, VA, May 2014.
4. H. Eldib, C. Wang, **M. Taha**, P. Schaumont 'QMS: Evaluating the side-channel resistance of masked software from source code,' The 51th Design Automation Conference (DAC-2014), June 2014.
5. **M. Taha**, P. Schaumont 'Differential Power Analysis of MAC-Keccak at Any Key-Length,' The 8th International Workshop on Security (IWSEC-2013), Okinawa, Japan, November 2013.
6. **M. Taha**, P. Schaumont 'A Key Management Scheme for DPA-Protected Authenticated Encryption,' Directions in Authenticated Ciphers (DIAC-2013), August 2013.
7. **M. Taha**, P. Schaumont 'Side-Channel Analysis of MAC-Keccak,' IEEE International Symposium on Hardware-Oriented Security and Trust (HOST-2013), June 2013 [nominated best paper].
8. **M. Taha**, P. Schaumont 'A Novel Profiled Side-Channel Attack in Presence of High Algorithmic Noise,' IEEE International Conference on Computer Design (ICCD-2012), September 2012.
9. S. Mane, **M. Taha**, P. Schaumont 'Efficient and Side-Channel-Secure Block Cipher Implementation with Custom Instructions on FPGA,' International Conference on Field Programmable Logic and Applications (FPL-2012), August 2012.
10. **M. Taha**, Y. Hasan, 'A Novel Headway-Based Vehicle-to-Vehicle Multi-Mode Broadcasting Protocol,' IEEE Vehicular Technology Conference (VTC-2008), September 2008.
11. **M. Taha**, Y. Hasan, 'VANET-DSRC Protocol for Reliable Broadcasting of Life Safety Messages,' IEEE International Symposium on Signal Processing and Information Technology (ISSPIT-07), December 2007.

Posters, Newsletters and Talks:

1. **M. Taha**'Lightweight Leakage Resiliency for Symmetric Cryptography,' Invited Talk at Northeastern University, September 2014.
2. **M. Taha** 'Advances in the Side-Channel Analysis of Symmetric Cryptography,' Invited Talk at Worcester Polytechnic Institute, July 2014.
3. **M. Taha**, P. Schaumont 'Side-Channel Analysis of MAC-Keccak,' Annual Workshop of Virginia Tech's Center for Embedded Systems for Critical Applications (CESCA), April 2013.
4. **M. Taha** 'The Birth of a New Hashing Standard: SHA-3,' CESCA Newsletter, February 2013.
5. **M. Taha**, P. Schaumont 'High Dimensional Leakage Modeling of Combinational Logic Circuits,' Annual Workshop of Virginia Tech's Center for Embedded Systems for Critical Applications (CESCA), May 2012.

AWARDS

- 2009-2013 Awarded a scholarship by the Egyptian Government to study the PhD Degree.
- 2004-2008 Awarded a scholarship to study the M.Sc Degree, Assiut University.
- 2004 Awarded Mobinil Company Research Grant.
- 2008 Awarded a travel grant to attend the Global Knowledge Forum NOOR-2008, Almadina, KSA.
- 2004 A scholastic rank of 2nd / 163 in the Bachelor Degree, Assiut University.

Activities

- 2013 Presentation at Directions in Authenticated Ciphers Workshop (DIAC-2013), Chicago IL.
- 2012 Attended the CRA-W Career Mentoring Workshop, Washington DC.
- 2011 Attended the Side-Channel Analysis Workshop at Cryptography Research, San Francisco CA.
- 2007 Session Chair in the IEEE ISSPIT'07, Cairo, Egypt.
- 2007 Faculty and Leadership Development Program, Assiut University.
- 2003 Training Workshop at Al Baath University, Syria.
- 2002 Training Workshop at Budapest Polytechnic, Hungary.
- 2001 Training Workshop at Warsaw University of Technology, Poland.

MEMBERSHIPS

- IACR Member since 2012
- IEEE Member since 2012

ACADEMIC SERVICES

Reviewer for journals:

- IEEE Transactions on Computers.
- IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.
- IEEE Transactions on Very Large Scale Integration Systems.
- ACM Transactions on Embedded Computing Systems.
- IACR Journal of Cryptographic Engineering.
- Elsevier Microprocessors and Microsystems.
- IEEE embedded systems letters.
- IET Circuits, Devices & Systems.

Reviewer for conferences:

- CHES'14, DATE'12,'14, HOST'13,'14,'15, COSADE'12,'14,'15, CARDIS'14, ReConFig'14, IWSEC'13, HASP'13, FPL'12, ISCAS'12.