RÉSUMÉ

PERSONAL DATA

Name:	Abdulhadi Shoufan
Nationality:	German

UNIVERSITY CAREER

1990-1995:	Study of electrical engineering at the University of Damascus, academic degree: Bachelor in Electronics
1998-2001:	Study of solid state electronics at the Technische Universität Darmstadt, academic degree: Dipl.-Ing
2001-2002:	PhD student in the Graduiertenkolleg „Electronic Commerce“ at the Technische Universität Darmstadt
2002-2007:	Continuation of the PhD study in the Integrated Circuits and Systems Lab at the Technische Universität Darmstadt
March 2007:	Attainment of the academic degree Dr.-Ing

OCCUPATIONAL CAREER

1995-1997:	Design engineer in the company Electric & Electronic Center in Homs-Syria
1997:	Research assistant in the department of Electrical Engineering at Albaath University in Homs-Syria
2002-2007:	Research assistant in the Integrated Circuits and Systems Lab at the Technische Universität Darmstadt
2007-2009:	Postdoctoral research and teaching fellow in the Integrated Circuits and Systems Lab at the Technische Universität Darmstadt
2008-2010:	Guest lecturer at Baden-Württemberg Cooperative State University, Stuttgart.
Since 2009:	Research team leader “Security Hardware” in the Center of Advanced Security Research Darmstadt, CASED.
2010-2011:	Assistant Professor at University of Sharjah UAE (College of Engineering, Computer Engineering, Embedded Systems).
Since Aug. 2011:	Assistant Professor for Information Security and ECE at Khalifa University.

FURTHER QUALIFICATIONS

Languages:	Arabic, German, English
EDP-Experience:	OS (MS Windows, Linux), programming languages (C/C++, Java), several modeling languages and CAD tools for the design and implementation of integrated circuits and systems

INTERESTS Music, sport, society and culture

Abdulhadi Shoufan

PUBLICATIONS

1. Abdulhadi Shoufan and Sumaya AlAmeri, “Natural Language Processing for Dialectical Arabic: A Survey”, ACL Workshop on Arabic Natural Language Processing, Beijing , China, July 2015.
2. Abdulhadi Shoufan, Hassan AlNoon, and Joonsang Baek, “On the Power Consumption of Cryptographic Processors in Civil Microdrones”, International Conference on Information Systems Security and Privacy, Loire Valley, France, February 2015.
3. Abdulhadi Shoufan, Zheng Lu, and Sorin Huss, “ A Web-based Visualization and Animation Platform for Digital Logic Design”, IEEE Transactions on Learning Technology, accepted and available as preprint.

1. Abdulhadi Shoufan, “A fault attack on a hardware-based implementation of the secure hash algorithm SHA-512”, IEEE International Conference on ReConFigurable Computing and FPGAs (ReConFig'13), December 2013.
2. Baek, J., Vu, Q., Shoufan, A., Jones, A., and Wong, D., “Stateful Public-Key Encryption Schemes Forward-Secure against State Exposure”, The Computer Journal, Vol. 56, Issue 4, 2013.
3. Noura Al Ebri, Joonsang Baek, Abdulhadi Shoufan, and Quang Hieu Vu, “Forward-Secure Identity-Based Signature: New Generic Constructions and Their Applications”, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). Vol. 4, No. 1, pp. 32-54, 2013.
4. Abdulhadi Shoufan, “A Hardware Security Module for Quadrotor Communication”, IEEE International Conference on Field-Programmable Technology (FPT'12) Dec. 2012.
5. Noura Al Ebri, Joonsang Baek, Abdulhadi Shoufan, and Quang Hieu Vu, “Efficient Generic Construction of Forward-Secure Identity-Based Signature”, The 7th International Conference on Availability, Reliability and Security. June 2012.
6. Tolga Arul and Abdulhadi Shoufan, “Consumer Opinions on Short-Interval Charging for Pay-TV over IPTV”, IEEE Conf. on Advanced Information Networking and Applications (AINA), Frontiers of Information Systems and Network Applications, March 2012.
7. Sunil Malipatlolla, Thomas Feller, Abdulhadi Shoufan, Tolga Arul, and Sorin A. Huss “A Novel Architecture for Secure Update of Cryptographic Engines on Trusted Platform Module”, IEEE International Conference on Field-Programmable Technology (FPT'11) Dec 2011.
8. Qizhi Tian, Abdulhadi Shoufan, Marc Stoettinger, and Sorin A. Huss “Power Trace Alignment for Cryptosystems featuring Random Frequency Countermeasures”, IEEE International Conference on Information Theory and Information Security (ICITIS2011) Nov. 2011.
9. Abdulhadi Shoufan and Tolga Arul “A Benchmarking Environment for Performance Evaluation of Tree-based Rekeying Algorithms”, The Journal of Systems and Software, Elsevier, 84, Page(s) 1130-1143, February 2011.
10. H. Gregor Molter, Marc Stöttinger, Abdulhadi Shoufan, and Falko Strenzke “A Simple Power Analysis on a McElice Cryptoprocessor”, Journal of Cryptographic Engineering, Springer, 1, Page(s) 29-36, January 2011.
11. Abdulhadi Shoufan, Nico Huber, and H. Gregor Molter “A Novel Cryptoprocessor Architecture for Chained Merkle Signature Scheme”, Microprocessors and Microsystems, Embedded Hardware Design, Elsevier, 35, Page(s) 34-47, February 2011.

12. Wang X., Shoufan A., and Huss S "A Quality of Service and Access Control Management for Batch Rekeying in Secure Multicast", International Conference on Internet Technology & Security (ITS 2010), November 2010.
13. Abdulhadi Shoufan and Tolga Arul, "Multicast Rekeying: Performance Evaluation", Book chapter in "Design Methodologies for Secure Embedded Systems", Springer 2010.
14. Abdulhadi Shoufan, Thorsten Wink, H. Gregor Molter, Sorin A. Huss, and Eike Kohnert, "A Novel Processor Architecture for McEliece Cryptosystem and FPGA Platforms", IEEE Trans. on Computers, Vol. 59, No. 11, Pages 1533-1546, November 2010. **Light spot paper.**
15. Stübing H., Shoufan A., and Huss S, "Enhancing Security and Privacy in C2X Communication by Radiation Pattern Control" IEEE International Symposium on Wireless Vehicular Communications (WIVEC 2010), Taipei, May 2010.
16. Stübing H., Shoufan A., and Huss S, "A Demonstrator for Beamforming in C2X Communication" IEEE International Symposium on Wireless Vehicular Communications (WIVEC 2010), Taipei, May 2010.
17. Abdulhadi Shoufan, Zheng Lu, and Guido Rößling, "A Platform for Visualizing Digital Circuit Synthesis with VHDL", 15th ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2010), 26-30 June, Ankara, Turkey.
18. Zheng Lu, Abdulhadi Shoufan, and Guido Rößling, "A Platform for VHDL Visualization", 8th European Workshop on Microelectronics Education (EWME 2010), 10-12 May, Darmstadt, Germany.
19. Abdulhadi Shoufan, "Analog and Mixed-Signal Modeling in VHDL-AMS", 8th European Workshop on Microelectronics Education (EWME 2010), 10-12 May, Darmstadt, Germany.
20. Abdulhadi Shoufan Nico Huber, "A Fast Hash Tree Generator for Merkle Signature Scheme", ISCAS2010, IEEE International Symposium on Circuits and Systems, Paris.
21. Abdulhadi Shoufan, "A Compact Course on VHDL-AMS", ISCAS2010, IEEE International Symposium on Circuits and Systems, Paris.
22. Shoufan A.,"An FPGA Accelerator for Hash Tree Generation in the Merkle Signature Scheme", 6th International Symposium on Applied Reconfigurable Computing ARC 2010.
23. Shoufan A. and Huss S., "Learning Outcomes Aligned Course on Reconfigurable Computing", 6th International Symposium on Applied Reconfigurable Computing ARC 2010.
24. Shoufan A. and Huss S., "A Course on Reconfigurable Computing", ACM Trans. on Computing Education. Vol. 10, Issue 2, pp. 7.1-7.20, June 2010.
25. Shoufan A., Stübing H., and Huss S, "Interactive Optimization of FPGA-based Systems-on-Chips", 13th GI/ITG/GMM Workshop "Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen", Feb 22-24, 2010, Dresden, Germany.
26. Shoufan A., Strenzke F., Molter G., and Stöttinger M.,"A Timing Attack Against Patterson Algorithm in the McEliece PKC", 12th International Conf. On Information Security and Cryptography, Seoul, Dec. 2009, LNCS 5461.
27. Shoufan A. and Huss S., "Understanding Physical Models in VHDL-AMS", IEEE Forum on Specification and Design Languages (FDL 2009), Sep. 2009, Sophia Antipolis, France.
28. Stübing H., Shoufan A., and Huss S, "Secure C2X Communication based on Adaptive Beamforming" 14. VDI International Conference on Electronic for Vehicles 2009.

29. Shoufan A. and Sorin A. Huss, “High-Performance Rekeying Processor Architecture for Group Key Management”, IEEE Trans. on Computers, Vol. 58, No. 10, Pages 1421-1434, October 2009.
30. Abdulhadi Shoufan, Thorsten Wink, H. Gregor Molter, Sorin A. Huss, and Falko Strenzke, “A Novel Processor Architecture for McEliece Cryptosystem and FPGA Platforms”, ASAP'09, 20th IEEE International Conference on Application-specific Systems, Architectures and Processors.
31. Israr A., Shoufan A., and Huss S., “An Efficient Reliability Evaluation Approach for System-Level Design of Embedded Systems”, IEEE Int. Symposium on Quality Electronic Design (ISQED'09).
32. Shoufan A., Stübing H., and Huss A, “OSCAR: Optimization of SoCs based on Computer-Aided Architecture Refinement” ACM/IEEE Design Automation and Test in Europe, DATE 2009, University Booth.
33. Adeel Israr, Abdulhadi Shoufan and Sorin A. Huss, “A Compact Error Model for Reliable System Design”, IEEE International Conference on High Performance Computing & Simulation (HPCS'09).
34. Shoufan A., Huss S., Kelm O., and Schipp S., “A Novel Rekeying Message Authentication Procedure based on Winternitz OTS and Reconfigurable Hardware Architectures” IEEE Int. Conference on Reconfigurable Computing (ReConFig 2008), Dec. 2008, Cancun, Mexico.
35. Strenzke F., Molter G., Tews E., Overbeck R., and Shoufan A., “Side Channels in the McEliece PKC”, Int. Workshop on Post Quantum Computer Cryptography PQCrypto, Lecture Notes in Computer Science, 5299/2008, Page(s) 216-229, Cincinnati, USA, October 2008.
36. Shoufan A. and Huss S. A., “Key Management in Secure Multicast”, GI Konferenz Sicherheit 2008: Sicherheit, Schutz und Zuverlässigkeit, Saarbrücken, April 2008. **Best paper award**. (In German)
37. Ugus O., Laue R., Westhoff D., Shoufan A., and Huss S. A., “Optimized Implementation of Elliptic Curve Based Additive Homomorphic Encryption for Wireless Sensor Networks”, Workshop on Embedded Systems Security, a workshop of the IEEE/ACM EMSOFT’2007 and the Embedded Systems Week, Salzburg, Austria, Oct. 2007.
38. Laue R., O. Kelm, S. Schipp, A. Shoufan, and Huss S.A., “Compact AES-based Architecture for Symmetric Encryption, Hash Function, and Random Number Generation” IEEE Conf. on Field Programmable Logic and Applications, FPL, Amsterdam, Netherlands, August 2007.
39. Shoufan A., “High Performance Group Key Management, A Way to scalable Internet Television”, VDM Verlag Dr. Müller, Saarbrücken, 2007, ISBN: 978-3-8364-2128-7.
40. Shoufan A., Laue R., and Huss S.A., “Reliable Performance Evaluation of Rekeying Algorithms in Secure Multicast” IEEE Int. Symposium on a World of Wireless, Mobile and Multimedia Networks, Helsinki, Finland, June 2007.
41. Shoufan A., Laue R., and Huss S.A., “High-Flexibility Rekeying Processor for Key Management in Secure Multicast” IEEE Int. Symposium on Embedded Computing SEC-07, Niagara Falls, Canada, May 2007.
42. Shoufan A., “Group Key Management: Algorithms, Benchmarking, and Reconfigurable Architectures” Dissertation, March 2007, http://elib.tu-darmstadt.de/diss/000814
43. Shoufan A., Laue R., and Huss S.A., “Secure Multicast Rekeying: A Case Study for HW/SW-Codesign” 10. Workshop “Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen”, Erlangen, Germany, March 2007.

44. Shoufan A. and Huss S., “Construction of a SPICE-similar Simulator for Education”, Analog’06, 8. GMM/ITG-Diskussionssitzung. Entwicklung von Analogschaltungen mit CAE-Methoden, Dresden, Germany, Sep. 2006.
45. Shoufan A. and Huss S.A., ”Rekeying Processor: A Scalable Solution for Group Key Management in Group Communication”, Thema FORSCHUNG, Technische Universität Darmstadt Ausgabe 1/2006, pp.86-89. (In German)
46. Shoufan A., Huss S., and Cutleriwala M., “A Novel Batch Rekeying Processor Architecture for Multicast Key Management”, Int. Conf. on High Performance Embedded Architectures & Compilers, LNCS 3793, pp. 169-183, Barcelona, Spain, Nov. 2005.
47. Shoufan A. and Sorin A. Huss, “Reduction of Structural Equation Set of Conservative VHDL-AMS Models”, Analog’05, 8. GMM/ITG-Diskussionssitzung. Entwicklung von Analog-schaltungen mit CAE-Methoden, Hannover, März 2005. (In German)
48. Shoufan A. and Sorin A. Huss, “Interactive Identification and Correction of Structural Modeling Errors in Conservative VHDL-AMS Models”, IEEJ International Analog VLSI Workshop, Macao, China Oct. 2004.
49. Shoufan A. and Sorin A. Huss, “A Scalable Rekeying Processor for Multicast Pay-TV on Reconfigurable Platforms”, Workshop on Application Specific Processors, IEEE/ACM Int. Conf. on Hardware/Software Codesign and System Synthesis, Stockholm, Sweden, Sep. 2004. **Best paper award.**

Supervised PhD, Diploma Master and Bachelor Theses

Internal Theses:

1. Abdelouahid Taadou, “Design of a Hardware Module for Encryption and Key Generation for a Rekeying Processor on a Reconfigurable Platform” Bachelor Thesis, 2004.
2. Peter Bungert, “Design of a Controller for the Rekeying Processor on a FPGA Platform”, Bachelor Thesis, 2004.
3. Bienvenu Tatsi, “Acceleration of Analog Simulation by Minimizing the Structural Equations in VHDL-AMS Models” Bachelor Thesis, 2004.
4. Zhaoming Dai ”Interactive Error Detection through Extraction of Mesh and Node Equations in Conservative VHDL-AMS Models”, Diploma thesis, 2004.
5. Murtuza Cutleriwala, “Batch Rekeying Processor on Reconfigurable Platform”, Master thesis, 2005.
6. Mojtaba Abrooy, “Dynamic Tree Management fort the Rekeying Processor, Analysis and Simulation” Bachelor Thesis, 2005.
7. Marcus Lindner und Joana Otetelisanu “Efficient Hardware Implementations of AES“, Bachelor Thesis, 2006.
8. Tobias Teichner, “HW/SW Design for the Rekeying Processor”, Diploma thesis, 2007.
9. Oliver Kelm und Sebastian Schipp, „Efficient Authentication of Rekeying Messages using Winternitz-OTS & Evaluation of several Rekeying Algorithms“ Diploma thesis, 2008.

10. Hagen Stübing, „IP-based Design of SoC“, Diploma thesis, 2008
11. Steve Kenfack Dongmo “A flexible Pay-TV System based on Multicast Rekeying: Client-Site“, Master thesis, 2008.
12. Liang Liang Zou, „A flexible Pay-TV System based on Multicast Rekeying: Server-Site“ Diploma thesis, 2008.
13. Thorsten Wink, “Quantum-Computer Resistant Cryptosystems: A FPGA-Implementation of McEliece”, Diploma thesis, 2009.
14. Nico Huber, “Quantum-Computer Resistant Cryptosystems: Design and Implementation of a Hardware Architecture for Merkle Signature Scheme”, Bachelor Thesis, 2009.
15. Zheng Lu and Pei Qian Li, “Visualization of VHDL Models Using ANIMAL: First Steps”, master thesis, 2009.
16. Kai Rohde, “Performance Optimization of the McEliece Cryptoprozessor on a Virtex-5 FPGA Platform” Master thesis, 2009.
17. Tolga Arul and Peter Müller, “Multicast Rekeying for Customer-Oriented IPTV” Diploma Thesis, 2009.
18. Elia Jehshan and Selami Kaya, “Conceptual Design of a Visualization Platform for Analysis and Simulation of Analog Systems” Diploma Thesis, 2009.
19. Eike Kohnert, “Modeling and Thynsesis of IP-based Systems on Transaction Level”, Diploma thesis 2010.
20. Nabil Sayegh, “Secure Communication and Picture Processing in Embedded Systems for Quadrocopters”, Diploma thesis 2010.
21. Noura Al-Ebri, “Leakage-Tolerant Identity-Based Signature for Mobile Devices”, Master thesis 2012.
22. Sumaya Al-Ameri, “A Web-based Lexicon Builder for Gulf Dialects” Master thesis 2014.
23. Sunil Malipatlolla, “A Novel Approach for a Flexible and Secure Update of Cryptographic Engines on a Trusted Platform Module”, PhD Thesis, 2013
24. Muhammed Al-Kuwaiti, “A Framework for Regulating The Cyberwar within the UAE”, Master thesis 2014.
25. Abdullah Albloushi, “The Implications of Social Media on the UAE National Security”, Master thesis 2015

Theses with Industry Collaboration:

26. Sven Rettig, “Conceptional Design of a Projection Display with Redundancy Architecture for Security Applications”, Diploma thesis, 2003. *Diehl in Frankfurt.*
27. Torsten Hahn, “Digital Parameter Recognition, Measurement Insecurity, and Wireless Transmission of Measurement Data in Multi-Component Receivers”, Diploma thesis, 2007. *GTM in Bickenbach.*
28. Subhrajit Roychowdhury „Developing a VHDL Editor Plug-in for Eclipse Based on Veditor“, Master thesis, 2008. *icHaus in Bodenheim.*

29. Johannes Felten „Data Maintaining in the Design of Integrated Circuits“, Diploma thesis, 2008. *icHaus in Bodenheim.*
30. Dominik Litzinger, “Design of a Phase-fired Rectifier for Power Supplies in Model Trains”, Bachelor Thesis 2008. *Massoth Elektronik in Seeheim.*

CURRENT RESEARCH AREAS

1. **Natural Language Processing**
    a. Building language resources for Arabic dialects
    b. Morphological and syntactical specification of the Emirati dialect

2. **Drone security**
    a. Behavioral analysis
    b. Communication security

3. **Pay-TV over IPTV**
    a. Customer oriented business model based on secure multicast rekeying
    b. Supporting heterogeneous groups

4. **Learning Technology**
    a. Visualization and animation
    b. Problem difficulty specification

5. **Security Hardware**
    a. High-Performance cryptoprocessor architectures, especially for post-quantum cryptography
    b. Side channel attacks

TEACHING OVERVIEW

At Technische Universität Darmstadt

1. Technical Foundations of Computer Science
2. Hardware Modeling Languages
3. Reconfigurable Processors
4. Modeling Heterogeneous Systems

The following commercial tools are deployed in the scope of these courses: PSPICE, ELDO (Mentor Graphics), Advance MS (Mentor Graphics), ActiveHDL (Aldec), SMASH (Dolphin), SynplifyPro (Synplicity), ISE (Xilinx) and EDK (Xilinx).

At Baden-Württemberg Cooperative State University (Stuttgart)

I have been responsible for the field of computer aided design with two lectures:

1. Design of Digital Systems
2. Modeling of Mixed Signal Systems

The University of Cooperative Education is characterized by high cooperation with more than 2000 companies and institutions which exercise students according to fixed contracts over the whole study time. More than 80% of students get a position at these companies after final degree. This model is highly successful and closes a wide gap between long study times at universities and the dynamic requirements of the German industry.

At University of Sharjah

1. Embedded Systems Design
2. Digital Logic Design
3. Real-time Embedded Systems

At Khalifa University for Science, Technology, and Research

1. Fundamental of Electronic Systems
2. Digital Logic Design
3. Real-time Embedded Systems
4. Introduction to Cryptography
5. Information Security Management
6. Operating Systems
7. Mathematics for Information Security
8. Research Methods in Engineering

Awards

Organization Name	Award	Date
Workshop on Application Specific Processors, IEEE/ACM Int. Conf. on Hardware/Software Codesign and System Synthesis	Best Paper Award	2004
Student council at department of computer science	Best Lecture Supervision: Modeling of Heterogeneous Systems	2005
Student council at department of computer science	Best Lecture Supervision: Reconfigurable Processors	2006
Gesellschaft für Informatik e.V. (Computer Science Society in Germany)	Best Paper Award	2008
Student council at department of computer science	Special Award for Merits in Education	2008
ASME	Third Place, Student Design Project Competition, Energy	2012

Special Qualifications

1. Cofounder and Academic Advisor of the Abu Dhabi Chapter of the Armed Forces Communications and Electronics Association (AFCEA).
2. Founder and leader of the research group Security Hardware at the Center for Advanced Security Research Darmstadt in Germany.
3. Industrial projects with diverse companies and institutions including
    a. Lockheed Martin Company (USA)
    b. Diehl Defence (Gemany)
    c. icHaus (Gemany)
    d. Massoth Electronics (Gemany)
    e. GTM (Gemany)
    f. Kobil and FlexSecure (Gemany)
    g. Adam Opel A (Gemany)
    h. German Federal Office for Information Security (Gemany)
4. Organization of several workshops and conferences such as the International Workshop on E-commerce in 2002 in Heidelberg and the FDL 2006 in Darmstadt.
5. Program committee member and reviewer in several conferences and journals.