

MUSAB A. ALTURKI

CONTACT INFORMATION

email musab.alturki@gmail.com
phone +1 (215) 470-7611
address 3508 Cypress Creek Rd,
Champaign, IL 61822, USA
Online profiles Website: musabalturki.net
LinkedIn: lnkd.in/CYGMTh
Google Scholar: goo.gl/UaXfZB
DBLP: dblp.org/pid/150/2827
Github: github.com/malturki

RESEARCH INTERESTS

Formal methods for program verification, specification and design of distributed and concurrent programming languages and systems, and for analysis of security properties.

EDUCATION

- Ph.D. in
Computer Science*
- 2006-2011 University of Illinois at Urbana-Champaign
Urbana, IL, USA · Department of Computer Science
- *Dissertation:* Rewriting-based Formal Modeling, Analysis and Implementation of Real-Time Distributed Services
 - *Committee:* José MESEGUER (Chair), Gul AGHA, Carl A. GUNTER, Grigore ROSU, Jayadev MISRA (UT Austin)
 - *Description:* Developed novel rewriting-based methods and tools for formally specifying distributed services, analyzing their properties and building correct-by-construction implementations.
- M.Sc. in
Computer Science*
- 2003-2005 University of Illinois at Urbana-Champaign
Urbana, IL, USA · Department of Computer Science
- *Thesis:* A Rewriting Logic Approach to the Semantics of Orc
 - *Advisor:* José MESEGUER
 - *Description:* Developed a provably correct, efficiently executable formal semantics of Orc applied to an online auction case study.
- B.Sc. in
Computer Science*
- 1997-2002 King Fahd University of Petroleum and Minerals
Dhahran, Saudi Arabia · Information & Computer Science Department
First Honors · GPA: 3.98 (Cumulative) and 4.0 (Major), both on a 4.0 scale

PROFESSIONAL EXPERIENCE

- RV Inc.*
- 2018–Present Senior Research Engineer
RUNTIME VERIFICATION INC. · Urbana, IL, USA
- Formal modeling and verification of safety and liveness properties in state-of-the-art decentralized consensus protocols (Ethereum’s Gasper and the Beacon Chain protocols, PlatOn’s Giskard protocol, and Algorand’s Pure PoS protocol)

- Statistical model checking of resilience of blockchain protocols against selective reveal attacks
- Design and development of correct-by-construction virtual machines for blockchain systems and verifying their correctness properties
- Formal modeling and analysis of Algorand’s smart contracts in TEAL/PyTEAL for conducting verification-oriented, industry-leading security audits

2017–2018 Visiting Research Scholar

UPenn

UNIVERSITY OF PENNSYLVANIA · Philadelphia, PA, USA

- Investigating formal methods for the design and analysis of secure cyber-physical systems and protocols
- Host: Andre SCEDROV, Chair of the Mathematics Department, Professor of Mathematics, Professor of Computer and Information Science

2013–2017 Assistant Dean of Research

KFUPM

KING FAHD UNIVERSITY OF PETROLEUM AND MINERALS · Dhahran, Saudi Arabia

- Strategic planning of research programs and activities
- Development and monitoring of research policies and regulations
- Administration of research grant applications, evaluations and operations
- Supervision of research support system development, including “Abhathi”, an enterprise research management system
- Management of four different units having a total of 20 employees

2011–2019 Assistant Professor

KFUPM

KING FAHD UNIVERSITY OF PETROLEUM AND MINERALS · Dhahran, Saudi Arabia

- Teaching introductory and advanced courses in computer science
- Conducting research in formal methods, programming languages and security
- Service through the development of courses and research programs, and contribution to the professional society

Summer 2008 Research Engineer Intern

DoCoMo Labs

DoCoMo USA LABS · Palo Alto, CA, USA

- Developed a framework based on Real-Time Maude for formal software specification and analysis including verification of non-functional timing properties of mobile software systems

2007–2011 Research Assistant

UIUC

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN · Urbana, IL, USA

- Developed formal methods and tools for the specification, analysis and implementation of real-time, distributed services
- Developed methods and tools for statistical analysis and model-checking of probabilistic systems, including analysis of resilience against DDoS and amplification attacks

2006–2007 Graduate Research Assistant

NCSA

NATIONAL CENTER FOR SUPERCOMPUTING APPLICATIONS · Urbana, IL, USA

- Investigated specifying role-based and attribute-based access control mechanisms using XML-based policy languages (such as XACML), and formally verifying their security properties using Margrave
- Extended the encryption techniques in the open-source Bouncycastle cryptography API in Java for secure e-mail and web services with a novel, two-staged identity-based encryption scheme

2002–2003 Database Developer and Administrator

KFUPM

KING FAHD UNIVERSITY OF PETROLEUM AND MINERALS · Dhahran, Saudi Arabia

- Developed and maintained a complete enterprise Microsoft SQL Server system for part-time job management, along with a dynamic, ASP-based web application front-end

2002–2003 Graduate Assistant

KFUPM

KING FAHD UNIVERSITY OF PETROLEUM AND MINERALS · Dhahran, Saudi Arabia

- Researched new network designs for VoIP applications and extensively analyzed them through deep OPNET simulations
- Taught introductory computer science labs in Java

Summer 2001 System Analyst Intern

Aramco

SAUDI ARAMCO · Dhahran, Saudi Arabia

- Managed various Sun Solaris 2.6/2.8 machines, configured production Sun SSP's and Clusters, and developed automation scripts in Perl

REFEREED PUBLICATIONS

An Extensible Compiler for Implementing Software Design Patterns as Concise Language Constructs

Oct. 2021

International Journal of Software Engineering and Knowledge Engineering (IJSEKE), Volume 31, Issue 7, pages 1043–1067, World Scientific
 Taher A. GHALEB, Khalid ALJASSER, Musab A. ALTURKI

Resource and timing aspects of security protocols

May 2021

Journal of Computer Security, Volume 29, Issue 3, pages 299–340, IOS Press
 Abraão AIRES URQUIZA, Musab A. ALTURKI, Tajana BAN KIRIGIN, Max KANOVICH, Vivek NIGAM, Andre SCEDROV and Carolyn TALCOTT

On Security Analysis of Periodic Systems: Expressiveness and Complexity

Feb 2021

Proceedings of the 7th International Conference on Information Systems Security and Privacy, ICISSP 2021, pages 43–54, SCITEPRESS
 Musab A. ALTURKI, Tajana BAN KIRIGIN, Max KANOVICH, Vivek NIGAM, Andre SCEDROV and Carolyn TALCOTT

Enhanced Visualization of Method Invocations by Extending Reverse-engineered Sequence Diagrams

Oct. 2020

Proceedings of 2020 Working Conference on Software Visualization (VISSOFT), 2020, pages 49–60
 Taher A. GHALEB, Khalid ALJASSER, Musab A. ALTURKI

Statistical Model Checking of RANDAO's Resilience to Pre-computed Reveal Strategies

August 2020

Proceedings of Formal Methods (FM) 2019 International Workshops, volume 12232 of Lecture Notes in Computer Science, pages 337–349
 Musab A. ALTURKI and Grigore ROSU

Towards a Verified Model of the Algorand Consensus Protocol in Coq

August 2020

Proceedings of Formal Methods (FM) 2019 International Workshops, volume 12232 of Lecture Notes in Computer Science, pages 362-367
 Musab A. ALTURKI, Jing CHEN, Victor LUCHANGCO, Brandon MOORE, Karl PALMSKOG, Lucas PENA and Grigore ROSU

Resource-Bounded Intruders in Denial of Service Attacks

June 2019

Proceedings of the 32nd IEEE Computer Security Foundations Symposium, pp. 382-396
 Abraão. URQUIZA, Musab A. ALTURKI, Max KANOVICH, Tajana BAN KIRIGIN, Vivek NIGAM, Andre SCEDROV and Carolyn TALCOTT

- A Multiset Rewriting Model for Specifying and Verifying Timing Aspects of Security Protocols*
 March 2019 Foundations of Security, Protocols, and Equational Reasoning - Essays Dedicated to Catherine A. Meadows, Lecture Notes in Computer Science, volume 11565, pp 192–213, Springer
 Musab A. ALTURKI, Tajana BAN KIRIGIN, Max KANOVICH, Vivek NIGAM, Andre SCEDROV and Carolyn TALCOTT
- Statistical Model Checking of Distance Fraud Attacks on the Hancke-Kuhn Family of Protocols*
 Oct. 2018 Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC@CCS'18), Toronto, ON, Canada, pp 60–71, ACM
 Musab A. ALTURKI, Max KANOVICH, Tajana BAN KIRIGIN, Vivek NIGAM, Andre SCEDROV and Carolyn TALCOTT
- Program Comprehension through Reverse-engineered Sequence Diagrams: A Systematic Review*
 June 2018 Journal of Software: Evolution and Process, Volume 30, Issue 11, e1965, Wiley
 Taher A. GHALEB, Musab A. ALTURKI, Khalid ALJASSER
- A Symbolic Rewriting Semantics of the COMPASS Modeling Language*
 Aug. 2017 IEEE 18th International Conference on Information Reuse and Integration, San Diego, CA, USA
 Musab A. ALTURKI
- Implementing the Observer Design Pattern as an Expressive Language Construct*
 Nov. 2015 The International Conference on Software Engineering Advances, Barcelona, Spain
 Taher A. GHALEB, Khalid ALJASSER, Musab A. ALTURKI
- Towards Formal Verification of Orchestration Computations Using the \mathcal{K} Framework*
 June 2015 Proceedings of the 20th International Symposium on Formal Methods (FM'15), Oslo, Norway, Lecture Notes in Computer Science, Volume 9109, pp 40–56, Springer
 Musab A. ALTURKI, Omar ALZUHAIBI
- Executable Rewriting Logic Semantics of Orc and Formal Analysis of Orc Programs*
 March 2015 Journal of Logic and Algebraic Methods in Programming: Special Issue on Automated Specification and Verification of Web Systems, Volume 84, Issue 4, pp 505–533, Elsevier
 Musab A. ALTURKI, José MESEGUER
- Sparse Single-hidden Layer Feedforward Network for Mapping Natural Language Questions to SQL Queries*
 Sep. 2014 Proceedings of the 24th International Conference on Artificial Neural Networks (ICANN'14), Hamburg, Germany, Lecture Notes in Computer Science, Volume 8681, pp 241–248, Springer
 Issam H. LARADJI, Lahouari GHOUTI, Faisal SALEH, Musab A. ALTURKI
- Stable Availability under Denial of Service Attacks through Formal Patterns*
 April 2012 Proceedings of Fundamental Approaches to Software Engineering (FASE'12), Tallinn, Estonia, Lecture Notes in Computer Science, Volume 7212, pp 78–93, Springer
 Jonas ECKHARDT, Tobias MÜHLBAUER, Musab A. ALTURKI, José MESEGUER, Martin WIRSING

- PVESTA: A Parallel Statistical Model Checking and Quantitative Analysis Tool*
 Aug. 2011 Proceedings of Algebra and Coalgebra in Computer Science (CALCO'11),
 Winchester, UK, Lecture Notes in Computer Science, Volume 6859, pp 386–392,
 Springer
 Musab A. ALTURKI, José MESEGUER
- DIST-ORC: A Rewriting-based Distributed Implementation of Orc with Formal Analysis*
 April 2010 Proceedings of the International Workshop on Rewriting Techniques for
 Real-Time Systems (RTRTS'10), Longyearbyen, Norway, Electronic Proceedings of
 Theoretical Computer Science, Volume 36
 Musab A. ALTURKI, José MESEGUER
- Model-Checking DoS Amplification for VoIP Session Initiation*
 Sep. 2009 Proceedings of the European Symposium on Research in Computer Security
 (ESORICS'09), Saint Malo, France, Lecture Notes in Computer Science, Volume
 5789, pp 390–405, Springer
 Ravinder SHANKESI, Musab A. ALTURKI, Ralf SASSE, Carl A. GUNTER, José
 MESEGUER
- Probabilistic Modeling and Analysis of DoS Protection for the ASV Protocol*
 Sep. 2009 Proceedings of the International Workshop on Security and Rewriting Techniques
 (SecReT'08), Pittsburgh, PA, USA, Electronic Notes in Theoretical Comp. Sci.,
 Volume 234, pp 3–18, Elsevier
 Musab A. ALTURKI, José MESEGUER, Carl A. GUNTER
- Formal Specification and Analysis of Timing Properties in Software Systems*
 March 2009 Proceedings of Fundamental Approaches to Software Engineering (FASE'09),
 York, UK, Lecture Notes in Computer Science, Volume 5503, pp 262–277,
 Springer
 Musab A. ALTURKI, Dinakar DHURJATI, Dachuan YU, Ajay CHANDER, Hiroshi
 INAMURA
- PBES: A Policy Based Encryption System with Application to Data Sharing in the Power Grid*
 March 2009 Proceedings of ACM Symposium on Information, Computer and Communications
 Security (ASIACCS'09), pp 262–275, Sydney, Australia, 2009, ACM
 Rakesh BOBBA, Himanshu KHURANA, Musab A. ALTURKI, Farhana ASHRAF
- Reduction Semantics and Formal Analysis of Orc Programs*
 May 2008 Proceedings of the International Workshop on Automated Specification and
 Verification of Web Systems (WWV'07), Venice, Italy, Electronic Notes in
 Theoretical Comp. Sci., Volume 200-3, pp 25–41, Elsevier
 Musab A. ALTURKI, José MESEGUER
- Real-time Rewriting Semantics of Orc*
 July 2007 Proceedings of the 9th International ACM SIGPLAN Conference on Principles and
 Practice of Declarative Programming (PPDP'07), pp 131–142, Wroclaw, Poland,
 2007, ACM
 Musab A. ALTURKI, José MESEGUER

ISSUED PATENTS

- SOURCE CODE COMPILER SYSTEM*
 Jan. 2021 Patent US010901712, USPO 2021
 Taher A. GHALEB, Khalid ALJASSER, Musab A. ALTURKI

- METHOD FOR COMPILING CONCISE SOURCE CODE*
 Jan. 2021 Patent US010901711, USPO 2021
 Taher A. GHALEB, Khalid ALJASSER, Musab A. ALTURKI
- REVERSE ENGINEERING METHOD, SYSTEM AND COMPUTER PROGRAM THEREOF*
 Feb. 2020 Patent US010552286, USPO 2020
 Taher A. GHALEB, Khalid ALJASSER, Musab A. ALTURKI
- METHODS, COMPUTER READABLE MEDIA, AND SYSTEMS FOR COMPILING CONCISE EXPRESSIVE DESIGN PATTERN SOURCE CODE*
 October 2019 Patent US010437572, USPO 2019
 Taher A. GHALEB, Khalid ALJASSER, Musab A. ALTURKI

INVITED TALKS

- Best Practices For Securing Algorand Smart Contracts*
 Nov. 2021 *Algorand Decipher*, Miami Light Project & the LAB Miami
 Miami, FL, USA
- Statistical Model Checking and Quantitative Analysis of Security Protocols*
 Dec. 2017 Protocol eXchange Meeting, National Cryptologic Museum,
 Annapolis Junction, MD, USA
- An Introduction to Rewriting Logic and the Maude Tool*
 June 2016 PL Club Seminar Series, University of Pennsylvania,
 Philadelphia, PA, USA
- Research Ethics*
 April 2015 University of Dammam,
 Dammam, Saudi Arabia
- Rewriting-based Formal Modeling and Analysis of Timed Distributed Services*
 Oct. 2011 CS Seminar Series, Carnegie Mellon University – Qatar,
 Doha, Qatar
- Rewriting Semantics and Formal Analysis of Orc Programs*
 Jan. 2010 Formal Methods Seminar, University of Texas,
 Austin, TX, USA

CONFERENCE TALKS

- On Security Analysis of Periodic Systems: Expressiveness and Complexity*
 Feb 2021 The 7th International Conference on Information Systems Security and Privacy
 (ICISSP'21)
 Vienna, Austria
- Enhanced Visualization of Method Invocations by Extending Reverse-engineered Sequence Diagrams*
 Sep. 2020 The 8th Working Conference on Software Visualization (VISSOFT'20)
 Adelaide, Australia
- Statistical Model Checking of RANDAO's Resilience to Pre-computed Reveal Strategies*
 Oct. 2019 The 1st Workshop on Formal Methods for Blockchains (FMBC'19)
 Porto, Portugal

- Oct. 2019 *Towards a Verified Model of the Algorand Consensus Protocol in Coq*
The 1st Workshop on Formal Methods for Blockchains (FMBC'19)
Porto, Portugal
- June 2019 *Resource-Bounded Intruders in Denial of Service Attacks*
The 32nd IEEE Computer Security Foundations Symposium (CSF'19)
Hoboken, NJ, USA
- March 2019 *A Multiset Rewriting Model for Specifying and Verifying Timing Aspects of Security Protocols*
Catherine Meadows Festschrift Symposium
Fredericksburg, VA, USA
- Oct. 2018 *Statistical Model Checking of Distance Fraud Attacks on the Hancke-Kuhn Family of Protocols*
The 2018 Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC @ CCS'18)
Toronto, ON, Canada
- July 2018 *Statistical Model Checking of Guessing and Timing Attacks on Distance-bounding Protocols*
The 15th Workshop on Foundations of Computer Security (FCS'18)
Oxford, UK
- Aug. 2017 *A Symbolic Rewriting Semantics of the COMPASS Modeling Language*
IEEE 18th International Conference on Information Reuse and Integration (IRI'17)
San Diego, CA, USA
- June 2015 *Towards Formal Verification of Orchestration Computations Using the \mathcal{K} Framework*
The 20th International Symposium on Formal Methods (FM'15)
Oslo, Norway
- Aug. 2011 *PVESTA: A Parallel Statistical Model Checking and Quantitative Analysis Tool*
Algebra and Coalgebra in Computer Science (CALCO'11)
Winchester, UK
- Sep. 2009 *Probabilistic Modeling and Analysis of DoS Protection for the ASV Protocol*
The International Workshop on Security and Rewriting Techniques (SecReT'08)
Pittsburgh, PA, USA
- March 2009 *Formal Specification and Analysis of Timing Properties in Software Systems*
Fundamental Approaches to Software Engineering (FASE'09)
York, UK

OTHER (SELECTED) PUBLICATIONS

- 2021 Tinyman Smart Contracts Audit Report · [Audit report](#)
- 2020 Formally Verifying Finality in Gasper: The Core of the Beacon Chain · [Blog post](#)
- 2020 Verifying Gasper with Dynamic Validator Sets in Coq · [Technical report](#)
- 2019 K vs. Coq as Language Verification Frameworks · [Blog post series](#)
- 2019 A Formal Model in K of the Beacon Chain: Ethereum 2.0's Primary Proof-of-Stake Blockchain · [Blog post](#)
- 2019 Formally Verifying Algorand: Reinforcing a Chain of Steel · [Blog post](#)

TEACHING

| | |
|--------------------|--|
| <i>Lecture</i> | THEORY AND DESIGN OF PROGRAMMING LANGUAGES · Graduate Fall 2014, Fall 2015, Fall 2016 · KFUPM, Saudi Arabia |
| <i>Lecture</i> | PRINCIPLES OF PROGRAMMING LANGUAGES · (Under)graduate Fall 2012, Fall 2013 · KFUPM, Saudi Arabia |
| <i>Lecture</i> | THEORY OF COMPUTATION · Undergraduate Spring 2012 · KFUPM, Saudi Arabia |
| <i>Lecture</i> | FORMAL METHODS AND MODELS IN SOFTWARE ENGINEERING · Undergraduate Fall 2011 · KFUPM, Saudi Arabia |
| <i>Lecture/Lab</i> | INTRODUCTION TO COMPUTING I & II · Undergraduate 2011 – 2013 · KFUPM, Saudi Arabia |
| <i>Lab</i> | INTRODUCTION TO COMPUTING I & II – LAB · Undergraduate Fall 2002, Spring 2003 · KFUPM, Saudi Arabia |

DISSERTATION

| | |
|----------------|--|
| <i>Title</i> | “Rewriting-based Formal Modeling, Analysis and Implementation of Real-Time Distributed Services” |
| <i>Summary</i> | My dissertation develops formal specification, simulation, prototyping, and analysis techniques and tools for distributed software services, based on rewriting logic, the Maude system, and the theory of Orc, with the overall goal of improving the reliability of <i>Internet software</i> , a class of distributed systems based on Internet-accessible software components. The dissertation focuses on two fundamentally important aspects of Internet software systems: (1) functional correctness of service compositions through reachability and model checking analysis (the web-based tool MORC) , and (2) availability of services (Quality-of-Service properties) through probabilistic modeling and statistical model checking and quantitative analysis (the client-server tool PVESTA). The notion of <i>stable availability</i> in cloud-based services, which guarantees a level of service regardless of how heavy a DDoS attack is, is introduced and defined through formal patterns. |

SOFTWARE AND PUBLIC REPOSITORIES

| | |
|----------|---|
| TEAL | Contributed 2021 · An extension of the static analysis tool Tealer to support TEAL versions 4 and 5 https://github.com/crytic/tealer |
| ETHEREUM | Developed 2020 · A formalization of the Ethereum’s Gasper protocol using Coq and K https://github.com/runtimeverification/beacon-chain-verification |
| ALGORAND | Developed 2019 · A formalization of the Algorand consensus protocol using the Coq proof assistant https://github.com/runtimeverification/algorand-verification |
| RANDAO | Developed 2018 · A probabilistic rewriting model of Randao-based random number generation schemes with statistical model checking https://github.com/runtimeverification/rdao-smc |
| MORC | Developed 2009-2011 · An online, web-based system for specifying and verifying service compositions, consisting of an interactive JQuery-based front-end and a PHP back-end powered by Maude http://www.ccse.kfupm.edu.sa/~musab/morc |
| PVESTA | Developed 2010-2011 · An efficient parallel statistical model checking and |

quantitative analysis tool written in Java
<http://maude.cs.uiuc.edu/tools/pvesta>

- IB-MKD Developed 2007-2008 · An open-source implementation of a novel policy-based encryption system as a modified Java Bouncycastle Library and its S/MIME and CMS Processors
- CAAC Developed 2001-2002 · A web-based, database-driven enterprise application for managing student part-time-job applications and processes

HONORS AND AWARDS

- 2021 *Kudos Award (twice)* · Runtime Verification Inc.
- 2014 *Distinguished Service Award* · College of Computer Science and Eng., KFUPM
- 2008 *Scholarship Award* · King Abdullah Scholar Award for Excellence in Research
- 2003 *Scholarship Award* · Higher Education Scholarship Award for Graduate Studies
- 2002 *First Honors* · First Honors Award in Computer Science
- 1997 *First Place* · Prince Muhammad bin Fahd's Award for Scientific Excellence

SELECTED PROFESSIONAL ACTIVITIES

- Security Audit Training* A team of 5 verification engineers · Formal modeling and analysis of Algorand smart contracts in TEAL/PyTEAL (2021)
- Graduate Student Supervision* Turki ALHAZMI · A formal system for computable financial contracts (Spring 2018)
- Shadi ALHAJ · A rewriting logic formalization of regular string transformations and formal analysis of transformation expressions (Spring 2017)
- Omar ALZUHAIBI · A Formal Semantics of Orc using the \mathcal{K} Framework and Formal Verification of Orc Programs (Fall 2016)
- Taher GHALEB · Improved Reverse Engineering Technique for Program Comprehension with Effective Sequence Diagrams (Spring 2016)
- PC and Review Board Membership* FTSCS 2012–2015 · International Workshop on Formal Techniques for Safety-Critical Systems
- SIMULTECH 2013, 2012 · International Conference on Simulation and Modeling Methodologies, Technologies and Applications
- SCP 2017, 2019 · Science of Computer Programming Journal
- JLAMP 2017 · Journal of Logical and Algebraic Methods in Programming
- FAC 2011 · Formal Aspects of Computing Journal
- JCS 2010 · Journal of Computer Security
- AMAST 2008 · International Conference on Algebraic Methodology and Software Technology
- Professional Affiliation* ACM 2014–PRESENT · Professional Member

SKILLS

- Programming* C/C++, Java, OCaml, Haskell, Perl, Bash, LaTeX
- Web* Javascript, JQuery, PHP, HTML5, CSS

Verification Maude, \mathcal{K} , Coq, Isabel/HOL, Java Modeling Language (JML), NuSMV, CVC4, Z3
Languages Fluent in both Arabic (native language) and in English

December 23, 2021