Ghada Almashaqbeh

Assistant Professor
University of Connecticut, CT, USA
Cell: +1 917-513-4507
Email: ghada.almashaqbeh@uconn.edu
Website: https://ghadaalmashaqbeh.github.io

RESEARCH INTEREST

I am interested in cryptography, computer systems security, and privacy. Broadly, I work on interdisciplinary projects that combine knowledge from various fields toward the design of secure systems and protocols. A large body of my work focuses on addressing security, privacy, and performance issues of blockchain-based systems and services. This is in addition to conceptual projects that aim to bridge the gap between theory and practice of cryptography.

EDUCATION

Columbia University **NY, USA** **2015 - 2019**
Ph.D. in Computer Science **2019**
M.Phil in Computer Science **2018**

- GPA: 4.21/ 4.0
- Research Interest: Cryptography, Computer Systems Security, and Privacy.
- Thesis: "CacheCash: A Cryptocurrency-based Decentralized Content Delivery Network."
  - Produced a startup (CacheCash Development Company, Inc.) that was founded in August 2018.
- Advisors: Allison Bishop and Tal Malkin.

University of Notre Dame **IN, USA** **2014 – 2015**
Ph.D. in Computer Science (Transfered to Columbia)
Computer Science and Engineering Department

- GPA: 4.0/4.0
- Research interest: Applied Cryptography and Privacy.
- Advisor: Marina Blanton

Jordan University of Science and Technology **Irbid, Jordan** **2006 - 2008**
M.Sc. in Computer Engineering

- GPA: 92.8%, ranked first among the enrolled students.
- Research interests: Wireless Networks.
- Thesis: "A Cross-Layer Based QoS Routing Framework for Wireless Mesh Networks."
- Advisors: Sameer Bataineh and Jamal Al-Karaki.

The Hashemite University **Zarqa, Jordan** **2001 - 2005**
B.Sc. in Electrical and Computer Engineering

- GPA: 3.94/4.00, ranked first among the enrolled students.
- Senior design project: "Building a Wireless Sensor Network (WSN) for Civil and Military Applications."
- Advisor: Jamal Al-Karaki.

Research Support

Submitted/Pending

- "Interoperability of Blockchain-Based Systems," Synchrony Financial, **$100K**. PI: Ghada Almashaqbeh (share **80%**), co-PI: Benjamin Fuller.

In Preparation

- "Towards Trustworthy and Performant Decentralized Resource Markets in the Blockchain Era," NSF SaTC: CORE, **$320K**. PI: Ghada Almashaqbeh.

PUBLICATIONS

In theory cryptography community authors are ordered in an alphabetic order, while in security/systems community authors are ordered based on contribution. Papers with alphabetic ordered author list are indicated with ** at the beginning.

Preprint / Under review

1. **G. Almashaqbeh** and R. Solomon, *"SoK: Privacy-Preserving Computing in the Blockchain Era,"* https://eprint.iacr.org/2021/727.pdf, Under review, 2021.
2. R. Solomon and **G. Almashaqbeh**, *"smartFHE: Privacy-Preserving Smart Contracts from Fully Homomorphic Encryption,"* https://eprint.iacr.org/2021/133, Under review, 2021.

Published

3. ** **G. Almashaqbeh,** F. Benhamouda, S. Han, D. Jaroslawicz, T. Malkin, A. Nicita, T. Rabin, A. Shah, E. Tromer, *"Gage MPC: Bypassing Residual Function Leakage for Non-Interactive MPC,"* in Proceedings of the 21st Privacy Enhancing Technologies Symposium (PETS), 2021. (Acceptance rate 19.7%)
4. **G. Almashaqbeh,** *"Rethinking Service Systems: A Path Towards Secure and Equitable Resource Markets,"* USENIX ;login: Magazine, 2021.
5. **G. Almashaqbeh**, A. Bishop, J. Cappos, *"MicroCash: Practical Concurrent Processing of Micropayments,"* in Proceedings of the 24th International Conference on Financial Cryptography and Data Security (FC), 2020.
6. **G. Almashaqbeh**, K. Kelley, A. Bishop, J. Cappos. *"CAPnet: A Defense Against Cache Accounting Attacks on Content Distribution Networks,"* in Proceedings of the 7th IEEE Conference on Communications and Network Security (CNS), 2019.

7. **G. Almashaqbeh**, A. Bishop, J. Cappos. *"ABC: A Cryptocurrency-Focused Threat Modeling Framework,"* in Proceedings of IEEE INFOCOM Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock), 2019. *BEST PAPER AWARD*
8. **G. Al-Mashaqbeh**, J. Al-Karaki, M. Al-Rousan, A. Raza, H. Abbas, and M. Pasha. *"Joint Geographic and Energy-aware Routing Protocol for Static and Mobile Wireless Sensor Networks."* Ad hoc & Sensor Wireless Networks 41, 2018.
9. Y. Zhang, M. Blanton, and **G. Almashaqbeh**. *"Implementing Support for Pointers to Private Data in a General-Purpose Secure Multi-Party Compiler."* ACM Transactions on Privacy and Security, 21(2), 2017.
10. J. Al-Karaki, **G. Al-Mashaqbeh**, and S. Bataineh. *"Routing protocols in wireless mesh networks: A survey."* International Journal of Information and Communication Technology 11, no. 4, 2017.
11. T. Hayajneh, B. Mohd, M. Imran, **G. Almashaqbeh**, and A. Vasilakos. "*Secure Authentication for Remote Patient Monitoring with Wireless Medical Sensor Networks,*" Sensors 16, no. 4, 2016.
12. Y. Zhang, M. Blanton, and **G. Almashaqbeh**. "*Secure distributed genome analysis for GWAS and sequence comparison computation,*" BMC Medical Informatics and Decision Making 15(Suppl 5), p. S4, 2015.
13. T. Hayajneh, **G. Almashaqbeh**, and S. Ullah. *"A green approach for selfish misbehavior detection in 802.11-based wireless networks,"* Mobile Networks and Applications, vol. 20, no. 5, 2015.
14. **G. Almashaqbeh**, T. Hayajneh, A. V. Vasilakos, and B. J. Mohd, *"QoS-Aware Health Monitoring System Using Cloud-Based WBANs,"* Journal of Medical Systems, vol. 38, no. 10, 2014.
15. T. Hayajneh, **G. Almashaqbeh**, S. Ullah, and A. V. Vasilakos, *"A Survey of Wireless Technologies Coexistence in WBAN: Analysis and Open Research Issues,"* Wireless Networks, vol. 20, no. 8, Springer US, pages 2165-2199, 2014.
16. T. Hayajneh,, R. Doomun, **G. Al-Mashaqbeh,** and B. J Mohd, *"An energy-efficient and security aware route selection protocol for wireless sensor networks,"* Security and Communication Networks, vol. 7, no. 11, pages 2015–2038, 2014.
17. T. Hayajneh, A. V. Vasilakos, **G. Almashaqbeh**, B. J Mohd, M. Shakir, K. Qaraqe and M. Imran, "*Public-Key Authentication for Cloud-based WBANs,*" in Proceedings of the 9th International Conference on Body Area Networks (BodyNets), 2014.
18. **G. Almashaqbeh**, T. Hayajneh, and A. V. Vasilakos. "A cloud-based interference-aware remote health monitoring system for non-hospitalized patients." in Proceedings of IEEE Global Communications Conference, 2014.
19. T. Hayajneh and **G. Al-Mashaqbeh,** "Multimedia traffic over WLANs: QoS support and performance evaluation," in Proceedings of the 5th IEEE International Conference on Information and Communication Systems (ICICS), Jordan, 2014.
20. **G. Al-Mashaqbeh**, "Computers and e-Health: Roles and new applications," in Proceedings of IEEE International Conference on Computer Systems and Industrial Informatics (ICCSII), UAE, 2012.

21. **G. Al-Mashaqbeh**, J. Al-Karaki, and S. Bataineh, *"CLEAR: A Cross-layer Enhanced and Adaptive Routing Framework for Wireless Mesh Networks,"* Wireless Personal Communications, vol. 51, no. 3, 2009.
22. J. Al-Karaki and **G. Al-Mashaqbeh**, *"SENSORIA: A New Simulation Platform for Wireless Sensor Networks,"* in Proceedings of IEEE International Conference on Sensor Technologies and Applications (SENSORCOMM), Spain, 2007.
23. J. Al-Karaki and **G. Al-Mashaqbeh**, *"Energy-Centric Routing in Wireless Sensor Networks,"* Elsevier Microprocessors and Microsystems, vol. 31, no. 4, 2007.
24. J. Al-Karaki and **G. Al-Mashaqbeh**, *"Energy-Centric Routing in Wireless Sensor Networks,"* in Proceedings of the 11th IEEE Symposium on Computers and Communications (ISCC), 2006.

Work in Progress

25. **G. Almashaqbeh**, A. Bishop, J. Cappos, *"CacheCash: A Cryptocurrency-based Decentralized Content Delivery Service."*
26. **G. Almashaqbeh**, Y. Erlich, J. Gershoni, T. Malkin, I. Pe'er, E. Tromer, *"Basing Cryptography on Biological Polymers."*

Posters

27. **G. Almashaqbeh**, *"Resistant and Scalable Storage Using Semi-Synthetic DNA,"* DARPA YFA PI Meeting, VA, Aug 2017.
28. **G. Almashaqbeh**, *"CacheCash: A Cryptocurrency-based Decentralized Content Delivery Service,"* New York Multidisciplinary Symposium on Security and Privacy, NYU Tandon School of Engineering, NY, Feb 2017.
29. **G. Almashaqbeh**, *"Mutual and Hierarchical Authentication Protocol for Cloud Assisted WBANs,"* Indiana Celebration of Women in Computing Conference (InWIC), Indianapolis, IN, Mar 2015.

TEACHING

Blockchain Technology

- Fall 2020, Fall 2021 - UConn CSE 5095 (Special Topics in Computer Science and Engineering). Course Homepage
- Summer 2019 - Fordham University CISC 6880.

Introduction to Computer and Network Security/Cybersecurity

- Spring 2021 - UConn CSE 3400/CSE 5850. Course Homepage

Independent Study in Security

- Fall 2020, Spring 2021 - UConn CSE 4099.

STUDENTS

Advising

PhD

- Zahra (Raha) Motaqy (Fall 2021 - present)

Undergraduate

- Bradshaw Pines Spring 2021, *On the role of blockchains in education systems.*
- Pablo Rodriguez 2020-2021, McNair Scholar, *Secure performance boosting of blockchain-based systems* → First job at Google.

Thesis Committee

- Justin Furuness - PhD at UConn.

HONORS AND AWARDS

- **2020:** Grace Hopper Celebration of Women in Computing (GHC) speaker - complementary registration.
- **2018:** Crypto 2018 student travel grant, Santa Barbara, CA.
- **2018:** CS PhD Service Award, Computer Science Department, Columbia University, NY.
- **2018:** Grossman Scholar Award, Fu Foundation School of Engineering and Applied Science, Columbia University, NY.
- **2017:** CRA-W Grad Cohort Workshop scholarship, Washington DC.
- **2016**: Grace Hopper Celebration of Women in Computing (GHC) student scholarship, Houston, TX.
- **2016:** CRA-W Grad Cohort Workshop scholarship, San Diego, CA.
- **2016:** Women in Theory Workshop scholarship, Berkeley, CA.
- **2015:** CRA-W Grad Cohort Workshop scholarship, San Francisco, CA.
- **2015:** Indiana Celebration of Women in Computing Conference (InWIC) scholarship, Indianapolis, IN.
- **2013:** First position in the 6th National Technological Parade, “Baby Care Assistant (BCA)” project, Jordan.
- **2011:** Second position in the International IT Competition at Zayed University, “3D Healthy Town” project, UAE.
- **2011:** Second position in the 4th National Technological Parade, for the “3D Healthy Town” project, Jordan.

- **2005:** Ranked 1st among enrolled students in the College of Engineering, and 2nd among the enrolled students in the Hashemite University, Jordan.
- **2005:** Senior design project sponsorship award, King Abdullah II Design and Development Bureau (KADDB) and the King Abdullah II Fund for Development (KAFD), Jordan.
- **2001 – 2005:** University and deanship honor list, the Hashemite University, Jordan.

TALKS AND PANELS

Talks

- "*Gage MPC: Bypassing Residual Function Leakage for Non-Interactive MPC.*"
  - Google Cryptography Talks Series - Jul 2021.
  - PETS 2021 - Jul 2021.
  - UConn CSE Security Seminar - Jul 2021.
- *"Rethinking Service Systems: A Path Towards Secure and Equitable Resource Markets."*
  - Grace Hopper Celebration (GHC), Security/Privacy track - Oct 2020.
- *"Micropayments: From Centralized to Blockchain-based Distributed Schemes."*
  - University of Malaga - May 2020.
- *"Building Secure Distributed Services and Resource Markets."*
  - University of Rochester - Mar 2020.
  - University of Florida - Mar 2020.
  - University of Connecticut - Mar 2020.
  - Georgetown University - Feb 2020.
  - University of Massachusetts at Lowell - Jan 2020.
- *"CAPnet: A Defense Against Cache Accounting Attacks on Content Distribution Networks."*
  - IEEE CNS'19 - June 2019.
- *"CacheCash: A Cryptocurrency-based Decentralized Content Delivery Network."*
  - PhD dissertation defense, Columbia University - May 2019.
- *"The Age of Cryptocurrencies: Bitcoin and Sisters:"*
  - University of Colorado Colorado Springs - Mar 2018 and Apr 2019.
  - NYU Tandon School of Engineering - Dec 2017.
  - Columbia University - Dec 2017.
- "*Threat Modeling for Cryptocurrency-based Systems.*"
  - NYU Tandon School of Engineering - Dec 2018.
- *"Resource-backed Cryptocurrencies:"*
  - Association of Women in Math (AWM) Talk Series, Barnard College - Nov 2018.
  - Emerging Scholars Program Seminar, Columbia University - Dec 2017.
- *"Sensible Cryptocurrencies."*
  - PhD Candidacy Exam Talk, Columbia University - Nov 2017.
- *"Cryptocurrency Era."*
  - Fordham University - Jun 2017.

- *"Bitcoin."*
  - NYU Tandon School of Engineering - Dec 2015.
- *"Digital Currencies."*
  - Cybersecurity for Teachers in Summer of STEM program, NYU Polytechnic School of Engineering - Jul 2015.

Panels

- *"Blockchain Coffee Talk,"* Synchrony Financial (SYF) - May 2021.
- *"Crypto-Economics 101,"* in the 6th Annual Entrepreneurship Festival *StartupColumbia*, Columbia University - Apr 2019.

PROFESSIONAL SERVICE

- **Service at UConn:**
  - Faculty search committee, CSE department at UConn, 2020/2021.
  - Strategic planning committee, CSE department at UConn, 2020/2021.
  - Judge for SDP (senior project design), Spring 2021.
  - Involved in organizing the CSE Security Seminar, Fall 2020.
- Ph.D coordinator of the Emerging Scholars Program (ESP) at Columbia University, Fall 2017 - Fall 2018.
- **Technical program committee:**
  - **Conferences:** Crypto 2021, IEEE HPSC 2016.
  - **Workshops:** CFAIL 2020, CFAIL 2019.
  - Applied Research Competition - NYU Cyber Security Awareness Week (CSAW 17, CSAW 16).
- **Reviewer/Sub-reviewer:**
  - **Conferences:** Eurocrypt 2021, Eurocrypt 2020, TCC 2018, USENIX Security 2018, DSC 2017, USENIX ATC 2017, Eurocrypt 2017, CCS 2016.
  - **Journals:** Journal of Human Rights, Springer Wireless Networks, IEEE Systems Journal, Wireless Personal Communication Journal, Journal of Medical Systems, Pervasive and Mobile Computing.
- **Professional membership:**
  - IACR (The International Association for Cryptologic Research).
  - ACM (Association for Computing Machinery).
  - WiCyS (Women in Cybersecurity).

WORK EXPERIENCE

Assistant Professor

University of Connecticut *CT, USA Aug 2020 – Present*

Computer Science and Engineering Department

Consultant

NuCypher *CA, USA Sep 2020 – Present*

- Looking into privacy preserving smart contracts.

Cryptographer

NuCypher *CA, USA Feb 2020 – Aug 2020*

- NuCypher is a startup that builds an infrastructure for privacy preserving applications.
- Worked on projects related to accounting attacks in the main network and privacy of smart contracts.

Cofounder and Research Scientist

CacheCash Development Company, Inc. *NY, USA*

Cofounder *Aug 2018 – Dec 2019*

Research Scientist *Jun 2019 – Dec 2019*

- CacheCash is a distributed content delivery service powered by a cryptocurrency, which is the core work of my PhD thesis.

Adjunct Instructor

Fordham University *NY, USA May 2019 – Aug 2019*

Computer Science Department

- *Teaching: Blockchain Technology Course*.

Graduate Research Assistant

Columbia University *NY, USA Sep 2015 – May 2019*

Computer Science Department

- Cryptography, security, privacy, and distributed computing.
- Advisors: Allison Bishop and Tal Malkin.

University of Notre Dame *IN, USA Aug 2014 – May 2015*

Computer Science and Engineering Department

- Applied cryptography and privacy.
- Advisor: Marina Blanton

Teaching Assistant

Columbia University *NY, USA Fall 2016*

Department of Computer Science *Fall 2017*

- Introduction to Cryptography Course.

Internships

New York University *NY, USA* *Jun – Jul 2015*
Computer Science and Engineering Department *Jun – Aug 2016*
Jul – Aug 2017

- Worked on the design and implementation of CacheCash.
- Advisor: Justin Cappos

Lecturer

The Hashemite University *Zarqa, Jordan*
Tutor (aka Lecturer) *Feb 2014 - Jul 2014*
Assistant Tutor (aka Assistant Lecturer) *Jun 2008 - Feb 2014*
Computer Engineering Department

- Teaching: C++ and object oriented programming, data structures, modeling and simulation, and digital logic design.
- Advising: Senior design projects, research .
- Research projects:
  - Energy-aware routing and joint security-routing algorithm for wireless sensor ad-hoc networks.
  - Coexistence issues and secure routing in wireless body area networks.

Lab Supervisor

The Hashemite University *Zarqa, Jordan* *Aug 2005 - Feb 2006*
Electrical and Computer Engineering Department
Microprocessors Lab

- Teaching: Electronic circuits, electrical circuits, and digital logic design labs.

REFERENCES

Tal Malkin
Associate Professor
Department of Computer Science, Columbia University, NY, USA
Phone: (212) 939-7097
Email: tal@cs.columbia.edu

Allison Bishop
President and Cofounder
Proof Trading, NY, USA
Email: allibishop@gmail.com

Thaier Hayajneh
University Professor

Department of Computer and Information Sciences, Fordham University, NY, USA
Phone: 212-636-7785
Email: thayajneh@fordham.edu

Eran Tromer
Associate Professor
School of Computer Science, Tel Aviv University, Tel Aviv, Israel
&
Associate Research Scientist
Department of Computer Science, Columbia University, NY, USA
Email: tromer@cs.tau.ac.il, eran@tromer.org