ANAS MELHEM

Tel: (+970)599320207 ⋄ E-mail: a.melhem@ptuk.edu.ps ⋄ Website: https://anas-melhem.github.io

SUMMARY

The Chair of the Computer Systems Engineering Department at Palestine Technical University. I have 15 years of extensive experience teaching undergraduate and graduate courses, including *Cryptography and Network Security*, *Software Security Engineering*, *Computer Networks*, and *Data Mining.* My research focuses on post-quantum cryptography, including designing novel cryptosystems like RCPKC, a faster and more secure alternative to NTRU, and conducting cryptanalysis on established schemes like RSA, NTRU, and HE1N. I have identified vulnerabilities in these systems and proposed countermeasures to enhance their security, contributing to the advancement of secure cryptographic solutions in the post-quantum era.

EDUCATION

- **PhD in Computer Engineering**
  Eastern Mediterranean University, North Cyprus. *September, 2021*
  - Thesis title: *Analysis and Development of Ciphers Homomorphic on Addition and Multiplication.*
  - Advisor: Prof. Dr. Alexander Chefranov.
- **Master's in Electronics and Computer Engineering**
  Al-Quds University, Palestine. *May, 2012*
  - Thesis title: *Ticket Authentication Wireless Mesh Networks Protocol.*
  - Advisor: Assoc. Prof. Dr. Rushdi Hamamreh.
- **Bachelor's in Electrical Engineering**
  Palestine Technical University, Palestine. *February, 2005*

ACADEMIC EXPERIENCE

Assistant Professor
Computer Systems Engineering Dept., Palestine Technical University *2021 – Present*

- Conducting pioneering research in post-quantum security.
- teaching courses in Cryptography and Network Security, Digital Logic Design, Data Mining, Discrete Mathematics, Operating Systems, and Computer Networks.
- Participating in multiple committees for revising course descriptions and preparing proposals for accrediting new programs.

Lecturer
Computer Systems Engineering Dept., Palestine Technical University *2016 – 2021*

- Taught various courses in Computer Systems Engineering Department.
- Participated in the Erasmus+ project titled "Pathway in Forensic Computing".

Research Assistant
Computer Engineering Dept., Eastern Mediterranean University, North Cyprus *2016 – 2018*

- Researched homomorphic cryptosystems.

- Taught several labs, including Operating Systems, Introduction to Programming, and Database Systems.
- Participated in a workgroup focused on preparing for ABET accreditation.

Lab Engineer
Computer Systems Engineering Dept., Palestine Technical University, *2009 – 2013*

- Instructing multiple labs including Digital Logic Design, Computer Architecture, Computer Networks, and Operating Systems.

RESEARCH & PROJECTS

Erasmus+ Project: Pathway in Forensic Computing

- Authored the chapter "*Digital Forensics Evidence Acquisition*" in the book **Digital Investigation Techniques and Tools**.
- Participated in technical workshops in Palestine and Jordan.

PhD Research Projects

- **Development of Post-Quantum Cryptosystem**: Developed RCPKC, a novel public key cryptosystem that is immune to lattice-based attacks and significantly faster than NTRU. It is particularly suitable for power-constrained devices.
- **RSA Security Analysis**: Developed a ciphertext-only attack using lattice basis reduction, effective against keys up to 8193 bits.
- **NTRU Cryptosystem Analysis**: Designed the NTRU modulo p flaw attack, with recommendations for parameter settings to mitigate the attack.
- **HE1N Cryptosystem Analysis**: Developed Known Plaintext Attacks (KPA) and ciphertext-only attacks (COA) against the HE1N cryptosystem, with new parameter settings to mitigate these attacks.

TEACHING EXPERIENCE

My journey in academia began in 2016 when I was promoted to lecturer in the Computer Systems Engineering Department at Palestine Technical University. Since then, I have instructed multiple undergraduate courses, including:

- 12140527 Cryptography and Network Security
- 12140420 Digital Logic Design
- 12140204 Discrete Mathematics
- 12140535 Data Mining
- 12140312 Computer Networks
- 12140308 Operating Systems

SKILLS

- Cryptographic Algorithm Design
- Cryptanalysis
- Curriculum Development
- Teaching and Mentoring

PROFESSIONAL DEVELOPMENT & MEMBERSHIPS

- Member of the committee for developing the Master's program in Software Engineering at Palestine Technical University.
- Participated in Erasmus+ workshops and projects focused on forensic computing and curriculum development.

PUBLICATIONS

Journal Papers

· Anas Ibrahim, Alexander Chefranov, Rushdi Hamamreh,"Ciphertext-Only Attack on RSA Using Lattice Basis Reduction", *The International Arab Journal of Information Technology*, vol. 18, no. 2, pp. 237 – 247, March. 2021.

· Anas Ibrahim, Alexander Chefranov, Nagham Hamad, Yousef-Awwad Daraghmi, Ahmad Al-Khasawneh, Joel J. P. C. Rodrigues,"NTRU-Like Random Congruential Public-Key Cryptosystem for Wireless Sensor Networks", *Sensors*, vol. 20, no. 16, pp. 4632 – 4657, Aug. 2020.

· Chuck Easttom, Anas Ibrahim, Alexander Chefranov, Izzat Alsmadi, Richard Hansen,"Towards A Deeper NTRU Analysis: A Multi Modal Analysis", *International Journal on Cryptography and Information Security (IJCIS)*, vol. 10, no. 2, pp. 11 – 22, Jun. 2020.

· Anas Ibrahim, Alexander Chefranov,"NTRU Modulo p Flaw", *International Journal for Information Security Research (IJISR)*, vol. 6, no. 3, pp. 685 – 690, Sep. 2016.

· Rushdi Hamamreh, Anas Melhem, "SWMPT: Securing Wireless Mesh Networks Protocol Based on Ticket Authentication", *The Research Bulletin of Jordan ACM*, vol. 2, no. 4, pp. 129 – 133, 2011.

· Rushdi Hamamreh, Anas Melhem, "Securing End-to-End Wireless Mesh Networks Ticket Based Authentication", *GSTF Journal on Computing (JoC)*, vol. 1, no. 2, 2011.

Conference Papers

· Anas Ibrahim, Alexander Chefranov, Nagham Hamad, "NTRU-Like Secure and Effective Congruential Public-Key Cryptosystem Using Big Numbers", in *Proc. 2019 2nd International Conference on new Trends in Computing Sciences (ICTCS), Amman, Jordan, 9-11 Oct. 2019.*

· Alexander Chefranov, Anas Ibrahim, "NTRU Modulo p Flaw", in *Proc. World Congress on Internet Security, WorldCIS 2016, London, UK, November 14-16, 2016.*

· Rushdi Hamamreh, Anas Melhem, "Secure Mobile Clients Using Elliptic Curve for WMN". in *Proc. The 13th International Arab Conference on Information Technology, ACIT 2012, Zarqa, Jordan, December 10-13, 2012.*

· Rushdi Hamamreh, Anas Melhem, "THWMP: A Ticket-Based Secure Hybrid Wireless Mesh Networks Protocol", in *Proc. 2011 Conference on Innovations in Computing and Engineering Machinery, CICEM2011, Amman, Jordan, September 5-7, 2011.*