Matluba Khodjaeva, PhD

CUNY John Jay College of Criminal Justice ● 524 W 59th St Office: 6.65.19● New York ● NY 10019 ● Tel. (212)237-8087 ● mkhodjaeva@jjay.cuny.edu

Professional Preparation

- **The Graduate Center, City University of New York (CUNY), New York, NY**
  - ***PhD and Master of Philosophy in Computer Science / Cryptography*** **2017**
    Dissertation Title: *"Secure and Efficient Delegation of a Single and Multiple Exponentiations to a Single Malicious Server"* Delaram Kahrobaei (advisor)
- **City College of New York, City University of New York (CUNY), New York, NY**
  - ***Master of Science in Computer Science*** **2017**
- **Hunter College, CUNY, New York, NY**
  - ***Master of Arts in Mathematics*** **2011**
  - ***Bachelor of Arts in Mathematics*** **2011**

Appointments

- **The Graduate Center, CUNY, New York, NY** **January 2019 - Present**
  Doctoral Faculty at PhD Program in Computer Science Department
- **John Jay College, CUNY, New York, NY** **September 2018 – Present**
  Assistant Professor in Computer Science & Mathematics Department and *Graduate Faculty at the Digital Forensics and Cybersecurity (D4CS)* in M.S. Degree program
- **John Jay College, CUNY, New York, NY** **January 2018 – September 2018**
  Adjunct Assistant Professor in Computer Science & Mathematics Department
- **York College, CUNY, New York, NY** **Spring 2018**
  Adjunct Assistant Professor in Computer Science & Mathematics Department
- **CUNY Research Foundation** **2016-2017**
  Research Assistant, PI: D. Kahrobaei, Research related to RFID, Cloud Cryptography
- **Brooklyn College, CUNY, New York, NY** **2011-2017**
  Adjunct Lecturer in Mathematics Department
- **Rutgers University, Newark, NJ** **2013-2018**
  Part Time Lecturer in Computer Science & Mathematics Department

Publications

Conference Papers:

1) G. Di Crescenzo, **M. Khodjaeva**, D. Kahrobaei, V. Shpilrain, *"On Single-Server Delegation of RSA Decryption"* in: CFail 2022, the Conference for Failed Approaches and Insightful Losses in Cryptology, Crypto 2022 LINK. (PDF file LINK)

2) G. Di Crescenzo, **M. Khodjaeva**, D. Kahrobaei, V. Shpilrain, *"A Survey on Delegated Computation"* in: 26th International Conference on Developments in Language Theory, DLT 2022. LINK. (PDF file LINK)

3) G. Di Crescenzo, **M. Khodjaeva**, V. Shpilrain, D. Kahrobaei and R. Krishnan, *"Single-Server Delegation of Ring Multiplications from Quasilinear-time Clients"*, in 14th International Conference on Security of Information and Networks (SINCONF 2021), 2021, pp. 1-8, LINK, (PDF file LINK)

4) G. Di Crescenzo, **M. Khodjaeva**, D. Kahrobaei, V. Shpilrain, "*Secure and Efficient Delegation of Pairings with Online Inputs"*, in: Liardet PY., Mentens N. (eds) Smart Card Research and Advanced Applications. CARDIS 2020. Lecture Notes in Computer Science, vol 12609. Springer, Cham (2020) LINK, (PDF file LINK).

5) G. Di Crescenzo, **M. Khodjaeva**, D. Kahrobaei, V. Shpilrain, "*Secure and Efficient Delegation of Elliptic-Curve Pairing"*, in: Conti M., Zhou J., Casalicchio E., Spognardi A. (eds) Applied Cryptography and Network Security. ACNS 2020. Lecture Notes in Computer Science, vol 12146. Springer, Cham (2020), Research Impact Score **4.46**, LINK, (PDF file LINK).

6) G. Di Crescenzo, **M. Khodjaeva**, D. Kahrobaei, V. Shpilrain, "*Delegating a Product of Group Exponentiations with Application to Signature Schemes"*, in: Conference Proceedings of the Number-Theoretic Methods in Cryptology Conference, (NuTMiC 2019), University of Sorbonne, Paris, 1- 23 (2019), (PDF file LINK).

7) M. Obaidat, **M. Khodjaeva**, S. Obeidat, D. Salane and J. Holst, "*Security Architecture Framework for Internet of Things (IoT)"*, in: 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 154-157 (2019), LINK. (PDF file LINK)

8) G. Di Crescenzo, **M. Khodjaeva**, D. Kahrobaei, V. Shpilrain, "*Secure Delegation to a Single Malicious Server: Exponentiation in RSA-type Groups"*, in: *2019 IEEE Conference on Communications and Network Security (CNS)*, Washington DC, DC, USA, 2019, pp. 1-9, LINK. (PDF file LINK)

9) G. Di Crescenzo, **M. Khodjaeva**, D. Kahrobaei, V. Shpilrain, "*Efficient and Secure Delegation to a Single Malicious Server: Exponentiation over Non-Abelian Groups"*, in: International Congress on Mathematical Software -- ICMS 2018, Lecture Notes Comp. Sc. 10931 (2018), 137—146, July 24-27, 2018, University of Notre Dame, Indiana, USA, LINK. (PDF file LINK)

10) G. Di Crescenzo, **M. Khodjaeva**, D. Kahrobaei, V. Shpilrain, "*Computing Multiple Exponentiations in Discrete Log and RSA Groups: From Batch Verification to Batch Delegation"*, in: 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, pp. 531-539 (2017), LINK. (PDF file LINK)

11) G. Di Crescenzo, **M. Khodjaeva**, D. Kahrobaei, V. Shpilrain, "*Practical and Secure Delegation of Exponentiations over Discrete-Log Groups to a Single Malicious Server"*, in: CCSW'17: Proceeding of the 2017 on Cloud Computing Security Workshop, pp 17-28 (2017), LINK. (PDF file LINK)

Journal Papers:

12) G. Di Crescenzo, **M. Khodjaeva,** D. Kahrobaei, V. Shpilrain, "*Delegating a Product of Group Exponentiations with Application to Signature Schemes"*, in: Journal of Mathematical Cryptology, De Gruyter 14, no. 1, 438-459, (2019-2020), Impact Factor **1.59**, LINK (PDF file LINK)

13) G. Di Crescenzo, **M. Khodjaeva**, D. Kahrobaei, V. Shpilrain, "*Efficient and Secure Delegation of Exponentiation in General Groups to a Single Malicious Server"*, in: Mathematics in Computer Science Journal, Springer 14, no. 3, 641-656 (2020), Impact Factor **1.15**, LINK (PDF file LINK)

14) M. Obaidat, I. Shahwan, A. Hassebo, S. Obeidat, M. Ali, **M. Khodjaeva**, "*SNR-Based Early Warning Message Scheme for VANETs",* in: Journal of Mobile Multimedia, Impact Factor **1.11**, pp. 163-190 (2020), LINK. **(Awarded as the best paper in Journal of Mobile Multimedia** LINK) (PDF file LINK)

Book Chapters:

15) M. Obaidat, **M. Khodjaeva**, J. Holst, M. Ben Zid, "*Security and Privacy Challenges in Vehicular Ad Hoc Networks"*, in: Mahmood Z. (eds) Connected Vehicles in the Internet of Things, Springer, Cham (2020), LINK (PDF file LINK)

16) **M. Khodjaeva**, M. Obaidat, D. Salane, "*Mitigating Threats and Vulnerabilities of RFID in IoT Through Outsourcing Computations for Public Key Cryptography",* in: Mahmood Z. (eds) Security, Privacy and Trust in the IoT Environment. Springer, Cham (2019), LINK (PDF file LINK)

PhD Thesis:

17) **M. Khodjaeva**, *"Secure Delegation of Exponentiations from Client to Single Malicious Server"*, (PhD thesis), in: The Graduate Center, CUNY Academic Works, NY (2017) LINK (PDF file LINK)

Accepted papers:

18) G. Di Crescenzo, **M. Khodjaeva**, Rajesh Krishnan, "Single-Server Delegation of Small-Exponent Exponentiation and Sum-Homomorphic Encryption from Quasilinear-time Clients", in: The ACM Conference on Computer and Communications Security (CCS), 3rd workshop in CPS&IoT Security and Privacy 2022.

19) M. Maras, S. Jain, H. Johnson, **M. Khodjaeva**, "*How Educational Institutions Can Help Fill the Cybersecurity Workforce Gap*", Security Management, Cybersecurity Talent Development Article.

Work in Progress:

20) Journal Paper: G. Di Crescenzo, **M. Khodjaeva**, D. Kahrobaei, V. Shpilrain, "*Secure Delegation of Exponentiations over Discrete-Log Groups and RSA type groups".*

21) Journal Paper: G. Di Crescenzo, **M. Khodjaeva**, D. Kahrobaei, V. Shpilrain, "*Batch Delegation of Exponentiation and Elliptic Curve Pairings".*

Grants

- Departmental nomination to 2023 Sloan Research Fellowship.
- PSC-CUNY- Grant 53, July 1, 2022 – June 30, 2023, "Secure and Efficient Delegation of Pairing with Membership Verification Test", CUNY Research Foundation Grant, **M. Khodjaeva** is PI, ($6,000).

- Advancement of Research (OAR) Faculty Scholarship Award, project name: *Secure and Efficient Delegation of Pairings and Algebraic Functions,* March 2022, $1500.
- NSF CISE-MSI: RCBP-ED: SaTC, Cultivating and Developing Research Talent to Support Research in Cyber-Security, with S. Jain (PI), **M. Khodjaeva** (Co-PI), M. Maras, H. Johnson, S. Graff (Co-PI), 2021-2023, $299,993.
- NSF 21-528 Campus Cyberinfrastructure, CC* Planning: Undertaking a Process that will Create a Comprehensive Blueprint for Improving Cyber-Infrastructure at John Jay College, CUNY, Member for application, with Anthony Carpi (PI), Shweta Jain (Co-PI), Marie-Helen Maras (Co-PI), **M. Khodjaeva** is a *Faculty Advisor*, 2021-2022, $100,000.
    - *Matluba Khodjaeva is a co-chair in the Software, Database and Simulation Applications Assessment Committee*
- Travel fund from Division of Mathematical Sciences from NSF ($1700)
- PSC-CUNY- Grant 52, July 1, 2021 – June 30, 2022, "Batch Pairing Delegation in Elliptic-Curve", CUNY Research Foundation Grant, **M. Khodjaeva** is PI, ($6,000).
- PSC-CUNY- Grant 51, July 1, 2020 – June 30, 2021, "Delegation of Elliptic-Curve Pairings", CUNY Research foundation Grant, **M. Khodjaeva** is PI ($6000).
- PSC-CUNY- Grant 50, July 1, 2019 – June 30, 2020, "Delegation of Group Exponentiation", CUNY Research foundation Grant, **M. Khodjaeva** is PI ($6,000).
- 2019-2020 Funded Research Faculty Development program, October 20, 2019 -- March 25, 2020, Project # 90671-00 08, ($1,500).
- 2019-2020 Inclusive Syllabus Seminar stipend, September 26, 2019 – May 7, 2020, ($1200).
- Faculty Travel Grant from John Jay College ($2,781.50), for the following conferences
    - ICMS 2018 ($1,000) in July 2018 and
    - AMS 2018 ($1,200) in October 2018
    - IEEE CNS, SPC 2019 ($581.50)
- NSF/ARO Student Travel Grant ($1000) for conference presentation IEEE, October 2017
- ONR, Research Assistantship, PI. D. Kahrobaei, ($7,500), March 2017.

Working in Progress:

- National Science Foundation, NSF SaTC, PI, "Delegation of Algebraic Operations in Cryptographic Protocols", with V. Shpilrain (Co-PI), 2021-2023, $353,575.

Honors and Awards

- Nominated for the 2022 John Jay College Distinguished Teaching Prize.

- Best Paper in Journal of Mobile Multimedia (JMM 2020), "SNR-Based Early Warning Message Scheme for VANETs", 2020.
- Tuition Fellowship, The Graduate Center, 2011-2016.
- Grad B Scholarship at Brooklyn College ($12,000 each year), 2012-2016.
- Dean's List, Hunter College, CUNY, 2008-2011.
- Golden Key Honor Society, 2008-2011.

Independent Study and PhD Thesis Advisor

PhD advisor of the following students:

1) PhD Thesis Advisor to Mohamed Ben Zid (PhD in Computer Science, CUNY Graduate Center, 2019)

2) PhD Thesis External Examiner, CUNY The Graduate Center, Di He, Advisor: Lei Xie, *"Learn Biological Meaningful Representations with Transfer Learning"*, Dissertation Proposal: March 1, 2021, Thesis: April 5, 2021.

3) PhD Thesis External Examiner, CUNY The Graduate Center, Ahmet Yuksel, Advisor: Robert Haralick, Proposal, ("*The N-tuple Subspace Method*"), Proposal: October 9, 2020, Oral Exam: May 30, 2020.

Undergraduate advisor of the following students:

4) Research study advisor for *Dilan Morales Caro* (starting 2022). Project name *is "Secure Multi Party Computation",* through OSRC (Office for Student Research & Creativity) scholarship.

5) Faculty Mentor CUNY Baccalaureate for Unique and Interdisciplinary Studies Area of Concentration (AOC) for Justin Plotsker, starting Fall 2021, majoring Computer Science and Cybersecurity.

6) Independent study advisor for Anastasiya Ayala (Summer 2, 2019). *"Implementation of Delegation of Cyclic Group Exponentiation in C++ and in Python"*

7) Independent study advisor for Fernando Cuevas (Summer 1, 2019). *"Secure Delegation of Exponentiation in RSA-type Groups and Implementation in C++ and in Python"*

Presentations in Conference and Research Meetings

- Association of Women in Mathematics 2022, AWM 2022 Research Symposium, "*Secure and Efficient Delegation of Pairings with Online Inputs*, June 16-19, 2022, University of Minnesota in Minneapolis, USA, LINK.
- SINCONF2021, 14th International Conference on Security of Information and Networks *"Single-Server Delegation of Ring Multiplications from Quasilinear-time Clients",* December 15-17, 2021, Edinburgh, Scotland and Gaziantep, Turkey, virtual conference due to COVID-19, LINK.

- Introduction Talk as the General Chair of the Conference in 42nd IEEE Symposium on Security and Privacy (IEEE S&P 2021), Systematic Approaches to Digital Forensic Engineering (SADFE 2021), May 27, 2021. LINK.
- CARDIS 2020, 19th Smart Card Research and Advanced Application Conference (2020) "*Secure and Efficient Delegation of Pairings with Online Inputs*, November 18-19, Germany, virtual conference due to COVID-19, LINK.
- Introduction Talk as the General Chair of the Conference in 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE 2020), virtual conference due to COVID-19, John Jay College, NY, LINK.
- Seminar Presentation at Computer Science Department at University of York, UK, July 8-11, 2019, presentation of conference papers in SPC 2019 and CCSW 2017.
- 2019 IEEE Conference on Communications and Network Security (CNS), "*Secure Delegation to a Single Malicious Server: Exponentiation in RSA-type Groups*, 5th IEEE Workshop on Security and Privacy in the Cloud, Washington DC, SPC, 2019, LINK.
- National Conference Talk, The American Mathematical Society, Special Session on Interactions between Algebra, Machine Learning and Data Privacy, "*Multiple Exponentiations in Discrete Log and RSA Groups*", October 2018, University of Michigan, Ann Arbor.
- International Conference Talk, ICMS 2018, Post-quantum Group-based Cryptography Session, "*Efficient and Secure Delegation to a Single Malicious Server: Exponentiation over Non-Abelian Groups*", July 24–27, 2018, University of Notre Dame, Indiana, USA, LINK.
- National Talk, American Mathematical Society, Special Session on Algorithmic Group Theory and Applications, "*Computing Multiple Exponentiations in Discrete Log and RSA Groups*", April 21–22, 2018, Northeastern University, Boston.
- 2017 Security and Privacy Day Conference, "*Computing Multiple Exponentiations in Discrete Log and RSA Groups*", October 2017, SUNY, New York.
- 2017 IEEE Conference on Communications and Network Security (CNS), "*Computing Multiple Exponentiations in Discrete Log and RSA Groups: From Batch Verification to Batch Delegation*" (October 2017), Las Vegas, Nevada.
- New York Multidisciplinary Symposium on Security and Privacy, "*Secure Delegation of Group Exponentiation to a Single Server*" (February 2017), New York University Tandon School of Engineering, Poster presentation.
- The Graduate Center, CUNY at Cryptography Student Seminar, "*Efficient and Secure Delegation of Group Exponentiation to a Single Server*" Part 1 (May 2016).
- The Graduate Center, CUNY at Cryptography Student Seminar, "*Efficient and Secure Delegation of Group Exponentiation to a Single Server*" Part 2 (July 2016).

Synergistic Activities

- Chair of committee to hire two computer science lecturers in the Department of Mathematics and Computer Science, John Jay College of Criminal Justice.

- Organizer of Association for Women in Mathematics 2022, AWM 2022, in Minneapolis, Minnesota for the 2022 Research Symposium, The Institute for Mathematics and its Applications, in partnership with the University of Minnesota, special session is *Mathematical Aspects of Cryptography*, June 16 –19, 2022. with D. Kahrobaei, LINK.
- Leading "Cryptography Research Group" in the department of Math and Computer Science at CUNY, John Jay College of Criminal Justice, since December 2021.
- Invited reviewer for the conference paper in 18th IMA International Conference on Cryptography and Coding (IMACC 2021).
- Faculty Administrative Liaison: Borough of Manhattan Community College (BMCC) and John Jay College dual degree program starting Fall 2021.
- Organizer and General Chair, Matluba Khodjaeva, 42nd IEEE Symposium on Security and Privacy (IEEE S&P 2021), Systematic Approaches to Digital Forensic Engineering (SADFE 2021), May 27, 2021, LINK.
- Organizer and General Chair, Matluba Khodjaeva, 13th Systematic Approaches to Digital Forensic Engineering (SADFE 2020), CUNY John Jay College of Criminal Justice, May 15, 2020, LINK.
- Computer Science Minor Coordinator at John Jay College of Criminal Justice, CUNY, since 2019.
- Member of the curriculum committee of the computer science and information security major, since Fall 2019.
- Member of the department committee on grade appeals and committee on faculty elections, since Fall 2020.
- Member of Undergraduate Research Initiatives in Science and Math (PRISM), since Fall 2019.
- Departmental academic advisor for Computer Science and Information Security (CSIS) major since Fall 2018.
- Made assessments for Cryptography and Cryptanalysis (CSCI 360) and Applied Cryptography (FCM 741) courses every year.
- Cryptography and Cryptanalysis (CSCI 360) course for each semester semesters since Fall 2018.
- Applied Cryptography (FCM 741) course for Fall 2020.
- Made curriculum development for the following courses: (1) Cryptography and Cryptanalysis (CSCI 360); (2) Discrete Mathematics (MAT 204) and (3) Applied Cryptography (FCM 741).
- Key technical consultant for Cryptography and Cryptanalysis at John Jay College.
- Organizer of laboratory (tutoring) sessions for Cryptography courses.

Courses Taught

- **John Jay College, CUNY, Mathematics and Computer Science Department:**
  - Cryptography and Cryptanalysis; Applied Cryptography; Mathematical Cryptography; and Independent Study.
- **The Graduate Center, CUNY, Mathematics and Computer Science Department:**
  - Independent Study on Research Project.

- **Brooklyn College, CUNY,** Mathematics Department:
    - Pre-Calculus A and B; Pre-Calculus; Calculus I; Thinking Mathematically; Elementary Mathematics from an Advanced Standpoint.
- **Rutgers University - Newark, Mathematics and Computer Science Department:**
    - Basic Calculus; Calculus I; Calculus III.
- **York College, CUNY, Mathematics and Computer Science Department:**
    - College Algebra; Introduction to Database Management.