

Nektarios Georgios Tsoutsos

Associate Professor, University of Delaware

E-mail: tsoutsos@udel.edu • web: udel.edu/~tsoutsos

Research Interests

- Applied Cryptography, Privacy Outsourcing, Hardware Security, Trustworthy Computing, Computer Architecture, Cyber-physical Systems

Education

- **Ph.D.** in Computer Science, New York University, New York, NY
Dissertation title: “*Private and Trustworthy Computation Using Additive Cryptographic Primitives*”
- **M.Sc.** in Computer Engineering, Columbia University, New York, NY
- **Diploma** (5-year) in Electrical and Computer Engineering, National Technical University of Athens, Greece

Academic and Leadership Appointments

- **Associate Professor**, ECE Department (primary) – CIS Department (joint), University of Delaware 09/25 –
- **Blockchain and Digital Innovation Task Force Member**, State of Delaware 05/26 –
- **Cyber Security Advisory Council Member**, State of Delaware 05/25 –
- **Co-Director**, FinTech Innovation Hub, University of Delaware 09/24 –
- **Associate Director**, Center for Cybersecurity, Assurance and Privacy (CCAP), University of Delaware 06/21 –
- **Assistant Professor**, ECE Department (primary) – CIS Department (joint), University of Delaware 09/18 – 08/25

Grants

- **Sole Principal Investigator:** [NSF SaTC 2239334] CAREER: Accelerating General-Purpose Encrypted Computation on Diverse Hardware 07/23 – 06/28
Sponsor: National Science Foundation (NSF), **Budget: \$534k**
- **Co-Principal Investigator:** [NSF DGE 2336586] CyberCorps Scholarship for Service: Defending Cyberspace through Active Learning (PI Barner) 01/24 – 12/28
Sponsor: National Science Foundation (NSF), **Budget: \$3.43M**
- **Co-Principal Investigator:** [NSF SaTC 2453861] SaTC: CORE: Medium: Verifiable Secure Hardware Design via Game-Theoretic and Cryptographic Primitives (PI Patnaik) 10/25 – 09/28
Sponsor: National Science Foundation (NSF), **Budget: \$600k**
- **Co-Principal Investigator:** [NSF DGE 2336586 supplement] Active Learning in Microelectronics: A Community Approach (PI Barner) 09/24 – 08/25
Sponsor: National Science Foundation (NSF), **Budget: \$337k**
- **Sole Principal Investigator (UD):** [NSF 2234974] Collaborative Research: Research Infrastructure: CCRI: New: Data-Driven Cybersecurity Research Infrastructure for Smart Manufacturing 04/23 – 03/26
Sponsor: National Science Foundation (NSF), **Budget: \$294k** (UD share as PI)
- **Sole Principal Investigator:** Student Experience with Mobile ID: Investigating how digital identification technologies reduce user friction in online services 06/22 – 12/24
Sponsor: Arkansas Venture Center/Discover Bank, **Budget: \$250k**
- **Sole Principal Investigator (UD/ECE):** [DE-EE0008768-006] Faster-than-real-time Simulation with Demonstration for Resilient DER Integration 11/19 – 10/23
Sponsor: Department of Energy (DoE)/Electrical Distribution Design, **Budget: \$253k** (UD/ECE share as PI)
- **Co-Principal Investigator:** Cybersecurity Certificate Program (PI Barner) 02/21 – 02/23
Sponsor: JPMorgan Chase, **Budget: \$450k**
- **Sole Principal Investigator:** Zilch: A Framework for Remote Verification of Security Properties using Zero Knowledge Proofs 06/21 – 06/23
Sponsor: University of Delaware Research Foundation, **Budget: \$38.5k**

- **Sole Principal Investigator (UD):** [NSF 1931916] *CPS: Medium: Collaborative Research: Frequency Domain Conversion of Computer Aided Design Files to Enable Encryption, Authentication and Feature Search Function* 09/19 – 08/21
Sponsor: National Science Foundation (NSF), **Budget:** \$165k (UD share as PI)

Professional Service

- **General Chair**
 - FinTech Technology Workshop '24
- **General co-chair**
 - *IEEE* Reliable and Resilient Digital Manufacturing (R2DM) Workshop '25, '24, '23, '21
- **Associate Editor**
 - *Elsevier* Journal of Information Security and Applications (JISA), editorial board member, '24 –
 - *IEEE* Embedded Systems Letters (ESL), editorial board member, '24 –
 - *IEEE* Embedded Systems Letters (ESL) '21 (special issue: Reliable and Resilient Digital Manufacturing)
- **Panel Reviewer**
 - *NSF* Secure and Trustworthy Cyberspace (SaTC) '26, '24, '23, '22
- **Organizing Committee**
 - Delaware FinTech Innovation Forum '26
 - Secure Delaware '26, '24, '23
 - Fintech and Financial Institutions Research Conference '25
 - *IEEE* International Conference on Computer Design (ICCD) '19
- **Track co-chair/coordinator**
 - Fintech and Financial Institutions Research Conference '25 (technical track)
 - *IEEE* Symposium on VLSI (ISVLSI) '24, '23, '22 (track: System Design and Security)
 - *IEEE* Hardware Oriented Security and Trust (HOST) '24 (track: Architecture Security)
- **External Review Committee**
 - *IEEE* International Symposium on Microarchitecture (MICRO) '22, '21, '20
- **Technical Program Committee**
 - *IEEE/ACM* International Conference on Computer-Aided Design (ICCAD) '26
 - *IEEE* International Symposium on Computer Architecture (ISCA) '26
 - *USENIX* Security Symposium '26, '25
 - *ACM* Asia Conference on Computer and Communications Security (AsiaCCS) '25
 - *IEEE* International Symposium on High-Performance Computer Architecture (HPCA) '25
 - *IEEE* Hardware Oriented Security and Trust (HOST) '26, '25, '24, '23
 - *IEEE* International Conference on Computer Design (ICCD) '26, '25, '24, '22, '21 (track: *Test, Verification, and Security*)
 - *IEEE* Symposium on On-Line Testing (IOLTS) '25, '24, '23
 - *ACM* Great Lakes Symposium on VLSI (GLSVLSI) '24, '23
 - *IEEE* International Symposium on Microarchitecture (MICRO) '23
 - *IEEE* MILCOM Artificial Intelligence for Cyber '23
 - *IEEE* ICCAD Top Picks in Hardware and Embedded Security (ICCAD-TPHES) '24, '23
 - *IEEE/ACM* Design Automation Conference (DAC) '21, '20 (track: *Hardware Security II: Attack and Defense*)
 - *IEEE* Symposium on VLSI (ISVLSI) '21, '20, '19 (track: *System Design and Security*)
 - *ACM* CPS & IoT Security and Privacy (CPSIoTSec) '21, '20
 - *Springer* Critical Infrastructure and Manufacturing System Security (CIMSS) '21
 - *IEEE/IFIP* Dependable Systems and Networks (DSN) '20
 - *IEEE* Asian Hardware Oriented Security and Trust (AsianHOST) '20, '19
 - *IEEE* International Conference on Computer Design (ICCD) '19 (track: *Processor Architecture*)
 - *IFIP/IEEE* International Conference on Very Large Scale Integration (VLSI-SoC) '19, '18 (track: *Hardware Security*)
- **External Reviewer**
 - *IEEE* International Symposium on Performance Analysis of Systems and Software ('25)
- **Technical Referee**
 - Proceedings of the *IEEE* ('25)
 - *IEEE* Transactions on Dependable and Secure Computing ('25)

- *Nature* Machine Intelligence ('25)
- *IEEE Transactions on Computers* ('25, '22, '20)
- *IEEE Transactions on Computer-Aided Design* ('25, '24, '23, '20, '19, '18)
- *IEEE Design & Test* ('24, '16)
- *ACM Computing Surveys* ('24)
- *ACM Digital Threats Research and Practice* ('23)
- *ASME Journal of Computing and Information Science in Engineering* ('23)
- *ACM Transactions on Architecture and Code Optimization* ('22, '21)
- *Springer Journal of Electronic Testing* ('22, '19)
- *IEEE Consumer Electronics Magazine* ('21)
- *IEEE Computer Architecture Letters* ('20)
- *IEEE Transactions on Mobile Computing* ('20)
- *Springer Journal of Cryptographic Engineering* ('20)
- *MDPI Cryptography* ('20)
- *Springer Journal of Ambient Intelligence and Humanized Computing* ('20, '19)
- *IEEE Micro* ('19)
- *IEEE Computer* ('19)
- *IEEE Access* ('19)
- *IEEE Embedded Systems Letters* ('19, '18)
- *IEEE Transactions on Information Forensics and Security* ('19, '17, '16)
- *IEEE Transactions on Emerging Topics on Computing* ('19, '18, '17)
- *Springer Journal of Hardware and Systems Security* ('17)
- *ACM Transactions on Design Automation of Electronic Systems* ('16, '15)
- *Springer Science China Information Sciences* ('16)
- *Elsevier Digital Signal Processing* ('17)
- *Elsevier Additive Manufacturing* ('17)
- *IET Electronics Letters* ('17)
- *Elsevier Journal of Information Security and Applications* ('16)
- **Technical Sub-reviewer**
 - *IEEE Transaction on Computer-Aided Design* ('19, '14)
 - *IEEE Transactions on Computers* ('16)
 - *IEEE Transactions on Information Forensics and Security* ('15, '14, '13)
 - *Elsevier Future Generation Computer Systems* ('15)
 - *ACM Transactions on Embedded Computing Systems* ('14)
 - *IEEE Transactions on Emerging Topics on Computing* ('13)
 - *IEEE/IFIP Dependable Systems and Networks* ('21)
 - *IEEE Hardware Oriented Security and Trust* ('20)
 - *Asia and South Pacific Design Automation Conference* ('19)
 - *IEEE International Symposium on Information Theory* ('19)
 - *IEEE VLSI Test Symposium* ('19, '17)
 - *ACM Asia Computer and Communications Security* ('18, '17)
 - *IEEE European Test Symposium* ('18)
 - *IEEE Symposium on VLSI* ('18, '16, '15, '14)
 - *IEEE International Test Conference* ('18, '17, '15, '14)
 - *IEEE Asian Hardware Oriented Security and Trust* ('17)
 - *IEEE International Symposium on On-Line Testing and Robust System Design* ('17, '16)
 - *IEEE/ACM Design Automation Conference* ('16, '15, '14)
 - *IEEE/ACM International Conference on Computer-Aided Design* ('16, '15)
 - *IEEE International Conference on Design & Technology of Integrated Systems* ('16, '14)

- *IEEE/ACM CASES: Compilers, Architectures and Synthesis for Embedded Systems* ('16, '15)
- *Great Lakes Symposium on VLSI* ('16)
- *Euromicro Digital System Design* ('16)
- *ACM Workshop on Cyber-Physical Systems Security & Privacy* ('15)
- *IEEE International Conference on Computer Design* ('13)
- **Session Chair/Moderator:**
 - *IEEE International Conference on Computer-Aided Design '24* (session: *Enhancing Simulation Efficiency through Multi-Core/GPU-Acceleration and Instruction-level Fault Injection*)
 - *IEEE Hardware Oriented Security and Trust '24* (session: *System Security*)
 - *IEEE Symposium on VLSI '22* (session: *Future Computing and Learning Techniques*)
 - *IEEE/EDAA Design Automation and Test in Europe '21* (session: *Attacks and defense mechanisms*)
 - *IEEE International Conference on Computer-Aided Design '20* (session: *Top Picks in Hardware and Embedded Security*)
 - *IEEE/ACM Design Automation Conference '19* (session: *Leaking like a Sieve: Exploits and Mitigations for Architecture Side Channels*)
 - *IEEE Hardware Oriented Security and Trust '19* (session: *(Anti)Reverse Engineering and Obfuscation*)
 - *IEEE International Conference on Computer-Aided Design '18* (sessions: *Designing and Assessing Secure Architectures, Approximate Computing*)
 - *IEEE International Conference on Computer-Aided Design '17* (session: *Synthesis and Security*)

Professional Affiliations

- **Senior Member**, Institute of Electrical and Electronics Engineers (IEEE) 05/25 –
- **Member**, Association for Computing Machinery (ACM) 01/23 –
- **Member**, International Association for Cryptologic Research (IACR) 04/22 –
- **Member**, Institute of Electrical and Electronics Engineers (IEEE) 10/18 – 04/25

University Service

- **Director**: Cybersecurity Minor, University of Delaware 04/23 –
- **Academic Advisor**: Computer Engineering Minor, University of Delaware 05/21 –
- **Academic Advisor**: CyberCorps Scholarship for Service, University of Delaware 09/24 –
- **Undergraduate Research Chair**: ECE Department, University of Delaware 01/22 – 09/22
- **Faculty Search Committee Chair**: ECE Department, University of Delaware 04/23 – 08/23
- **Faculty Search Committee**: ECE Department, University of Delaware 09/22 – 03/23
- **Faculty Search Committee**: ECE Department, University of Delaware 09/18 – 07/19
- **Graduate Committee**: ECE Department, University of Delaware 09/18 – 08/22
- **Undergraduate Committee**: ECE Department, University of Delaware 02/24 – 08/24
- **Cybersecurity Steering Committee**: ECE Department, University of Delaware 09/19 – 08/20
- **Training Working Group**: Data Science Institute, University of Delaware 03/25 –
- **Examiner**: Qualifying Exam, ECE Department 07/21 –
- **Qualification Exam Ad-Hoc Committee**: ECE Department, University of Delaware 10/21 – 05/22
- **NSF REU Site Mentor**: ECE Department, University of Delaware 06/23 – 08/25
- **Marketing Committee**: ECE Department, University of Delaware 08/25 – 05/26

Community Service and Global Outreach

- **Faculty Leader/Organizer**: Embedded Systems Challenge, Cyber Security Awareness Worldwide 01/19 –
- **Faculty Co-Organizer**: Capture the Flag, UD Center for Cybersecurity, Assurance and Privacy 01/21 –
- **Challenge Leader/Organizer**: Embedded Systems Challenge, Cyber Security Awareness Worldwide 06/15 – 11/17
- **External Advisor**: Advanced Placement (AP) Research course, Newark Charter High School 09/21 – 05/22

Teaching

- **University of Delaware, ECE Department**

<i>CPEG 475/675 - IoT and Embedded Systems Security</i>	Spring 2019
<i>CPEG 475/675 - IoT and Embedded Systems Security</i>	Fall 2019
<i>CPEG 472/672 - Applied Cryptography</i>	Spring 2020
<i>ELEG 662 – Digital Systems Seminar</i>	Spring 2020
<i>CPEG 475/675 - IoT and Embedded Systems Security</i>	Fall 2020
<i>CPEG 472/672 - Applied Cryptography</i>	Spring 2021
<i>CPEG 697 - Advanced Cybersecurity [JPMC Certificate]</i>	Fall 2021
<i>CPEG 475/675 - IoT and Embedded Systems Security</i>	Fall 2021
<i>CPEG 472/672 - Applied Cryptography</i>	Spring 2022
<i>ELEG 662 - Digital Systems Seminar</i>	Spring 2022
<i>CPEG 697 - Advanced Cybersecurity [JPMC Certificate]</i>	Fall 2022
<i>CPEG 472/672 - Applied Cryptography</i>	Spring 2023
<i>ELEG 666 - Independent Study</i>	Spring 2023
<i>CPEG 472/672 - Applied Cryptography</i>	Fall 2023
<i>CPEG 365/465 - Introduction to Cybersecurity Engineering</i>	Spring 2024
<i>CPEG 666 - Independent Study</i>	Summer 2024
<i>CPEG 472/672 - Applied Cryptography</i>	Fall 2024
<i>CPEG 467/667 – Career and Success Development [NSF SFS]</i>	Fall 2024
<i>CPEG 365 - Introduction to Cybersecurity Engineering</i>	Spring 2025
<i>CPEG 467/667 – Career and Success Development [NSF SFS]</i>	Spring 2025
<i>CPEG 472/672 - Applied Cryptography</i>	Fall 2025
<i>CPEG/ELEG/CISC/MISY 465/665 - Introduction to Cybersecurity</i>	Fall 2025
<i>CPEG 406/606 – Career and Success Development [NSF SFS]</i>	Fall 2025
<i>CPEG 365 - Introduction to Cybersecurity Engineering</i>	Spring 2026
<i>CPEG 406/606 – Career and Success Development [NSF SFS]</i>	Spring 2026

Doctoral Committees

- **Dimitris Mouris**, "*Private and Verifiable Computation*," University of Delaware, ECE Department, December 2023 (Committee Chair)
- **Fatema Bannat Wala**, "*The State of The Art in DNS Security and its Implications*," University of Delaware, ECE Department, June 2023 (Committee Member)
- **Charles Gouert**, "*Efficient General-Purpose Computation with Fully Homomorphic Encryption*," University of Delaware, ECE Department, July 2023 (Committee Chair)
- **Lars Folkerts**, "*Improving the Efficiency and Security of Fully Homomorphic Machine Learning as a Service*," University of Delaware, ECE Department, May 2025 (Committee Chair)
- **Ehsan Memary**, "*Security With Decentralization*," University of Delaware, CIS Department, April 2026 (Committee Member)

Advisees and Interns

University of Delaware

- **Rostin Shokri**, Ph.D. student – University of Delaware, Trustworthy Computing Group 09/23 –
- **Omar Ahmed**, Ph.D. student – University of Delaware, Trustworthy Computing Group 09/24 –
- **Kashfia Farheen**, Ph.D. student – University of Delaware, Trustworthy Computing Group 09/25 –
- **Sakib Anwar**, Ph.D. student – University of Delaware, Trustworthy Computing Group 09/25 –

- **Anish Chakraborty**, Independent Research Student – Charter School of Wilmington, DE 11/24 –
- **Katina Thongvong**, M.Sc. student – University of Delaware, Trustworthy Computing Group 01/25 –
- **Lars Folkerts**, Ph.D. student – University of Delaware, Trustworthy Computing Group 06/20 – 02/26
- **Christos Madamopoulos**, REU scholar – University of Delaware, Trustworthy Computing Group 06/25 – 08/25
- **Mariel Diaz**, REU scholar – University of Delaware, Trustworthy Computing Group 06/25 – 08/25
- **Julian Lenis**, Graduate intern – University of Delaware, Trustworthy Computing Group 06/25 – 08/25
- **Oscar Hernan Olaya Gutierrez**, Ph.D. student – University of Delaware, ECE Department 01/24 – 06/25
- **Sasidhar Kunapuli**, Independent Research Student – Lynbrook High School, Santa Clara, CA 08/24 – 05/25
- **Jack Cartwright**, Undergraduate student – University of Delaware, Trustworthy Computing Group 06/24 – 12/24
- **Charles Gouert**, Ph.D. student – University of Delaware, Trustworthy Computing Group 09/18 – 09/24
- **Christos Madamopoulos**, REU scholar – University of Delaware, Trustworthy Computing Group 06/24 – 08/24
- **Melqui Aguirre**, Graduate intern – University of Delaware, Trustworthy Computing Group 06/24 – 08/24
- **Omar Ahmed**, M.Sc. student – University of Delaware, Trustworthy Computing Group 09/23 – 08/24
- **SuoAn Gao**, Ph.D. student – University of Delaware, ECE Department 09/23 – 03/24
- **Dimitris Mouris**, Ph.D. student – University of Delaware, Trustworthy Computing Group 01/19 – 02/24
- **Jhan Carlos Diaz Vidal**, Graduate intern – University of Delaware, Trustworthy Computing Group 06/23 – 12/23
- **Brandon Bauer**, REU scholar – University of Delaware, Trustworthy Computing Group 06/23 – 08/23
- **Mihailo Knezevic**, Graduate intern – University of Delaware, Trustworthy Computing Group 06/23 – 08/23
- **Brandon Cox**, Graduate independent study, University of Delaware, ECE Department 04/23 – 06/23
- **Ethan Conway**, Undergraduate student – University of Delaware, Trustworthy Computing Group 06/22 – 08/22
- **Paul Zaloga**, Undergraduate student – University of Delaware, Trustworthy Computing Group 06/22 – 08/22
- **Anusha Devisetty**, AP Research student – Newark Charter High School, DE 09/21 – 05/22
- **Nicholas Kater**, Undergraduate student – University of Delaware, Trustworthy Computing Group 07/20 – 08/21
- **Manish Chaudhary**, M.Sc. student – University of Delaware, Trustworthy Computing Group 09/19 – 05/21
- **Ryan Peterson**, Undergraduate student – University of Delaware, Trustworthy Computing Group 07/19 – 08/19
- **Maggie McGrath**, Undergraduate student – University of Delaware, Trustworthy Computing Group 01/19 – 02/19

New York University

- **Dimitris Mouris**, Graduate student (remote) – University of Athens 02/17 – 11/17
- **Abhinay Kumar**, Undergraduate summer intern (remote) – IIT Kanpur 05/17 – 07/17
- **Homer Gamil**, Undergraduate summer intern – New York University 05/16 – 06/16 and 05/17 – 06/17
- **Yilkal Abe**, Postgraduate summer research assistant – New York University 05/16 – 08/16
- **Dimitrios Tychalas**, Graduate research assistant – New York University 12/15 – 08/16

Honors and Awards

- **National Science Foundation (NSF) CAREER Award** (Secure & Trustworthy Cyberspace program) 07/23
- **Recognition: Delaware's 15 Most Influential Business Leaders** in 2023 by the Delaware News Journal 04/23
- **University of Delaware Research Foundation (UDRF) Award** 06/21
- **Pearl Brownstein Doctoral Research Award** for doctoral research showing the greatest promise (NYU) 05/18
- **New York University Ph.D. Student Fellowship** 01/13 – 12/17
- **Deborah Rosenthal Award** for outstanding performance on the Ph.D. Qualification Exam (NYU) 05/14
- **1st Place Award** at CSAW Embedded Security Challenge for the design of stealthy hardware Trojan horses 11/13
- **Advisee Honor: 1st Place Award** at CSAW Embedded Security Challenge for designing IoT covert channels (C. Gouert) 11/18
- **Advisee Honor: Graduate Fellowship** by Gerondelis Foundation (D. Mouris) 11/20
- **Advisee Honor: 3rd Place Award** at CSAW Hack3D for reverse engineering additive manufacturing files (N. Kater) 11/20

- **Advisee Honor: 1st Place Award** at ECE Research Day for privacy-preserving neural network inference (L. Folkerts and C. Gouert) 05/21
- **Advisee Honor: Graduate Faculty Award** on Computer Systems & Networks (C. Gouert) 05/21
- **Advisee Honor: 1st Place Best Presentation Award** at *IEEE R2DM Workshop* (D. Mouris) 09/21
- **Advisee Honor: 2nd Place Best Presentation Award** at *IEEE R2DM Workshop* (L. Folkerts) 09/21
- **Advisee Honor: Graduate Block Funding Fellowship** of ECE department (C. Gouert) 11/21
- **Advisee Honor: Graduate Student Excellence in Teaching Award** of UD College of Engineering (L. Folkerts) 04/22
- **Advisee Honor: 1st Place Award** at ECE Research Day for privacy-preserving multi-exit neural networks (L. Folkerts) 05/22
- **Advisee Honor: Graduate Fellowship Finalist** by NVIDIA (C. Gouert) 11/22
- **Advisee Honor: Doctoral Fellowship for Excellence** of UD Graduate College (C. Gouert) 02/23
- **Advisee Honor: Travel Grant** from NDSS 2023 Symposium (L. Folkerts) 03/23
- **Advisee Honor: Travel Grant** from PETS 2023 Symposium (D. Mouris) 05/23
- **Advisee Honor: 1st Place Award** at ECE Research Day for Accelerated Encrypted Computing on GPUs (C. Gouert) 05/23
- **Advisee Honor: First-year Scholarship** of ECE department (O. Gutierrez) 02/24
- **Advisee Honor: ECE Faculty Award** for Computer Engineering (L. Folkerts) 05/24
- **Advisee Honor: Builder Bounty 2024 Award** by Nillion for secure biometric authentication using private facial recognition (O. Ahmed, L. Folkerts) 08/24
- **Advisee Honor: Best Paper Award Candidate** at the IEEE ICCD 2025 conference (R. Shokri) 11/25

Doctoral Dissertation Supervisor

[D1] **D. Mouris**, "Private and Verifiable Computation," *Ph.D. Dissertation*, University of Delaware, Newark, Delaware 19716, December 2023. (Primary advisor: N. Tsoutsos)

[D2] **C. Gouert**, "Efficient General-Purpose Computation with Fully Homomorphic Encryption," *Ph.D. Dissertation*, University of Delaware, Newark, Delaware 19716, July 2024. (Primary advisor: N. Tsoutsos)

[D3] **L. Folkerts**, "Improving the Efficiency and Security of Fully Homomorphic Machine Learning as a Service," *Ph.D. Dissertation*, University of Delaware, Newark, Delaware 19716, January 2026. (Primary advisor: N. Tsoutsos)

Master's Thesis Supervisor

[M1] **O. Ahmed**, "Verifiable Encrypted Computations," *Master's Thesis*, University of Delaware, Newark, Delaware 19716, July 2024. (Primary advisor: N. Tsoutsos)

Scholarly Works

[An asterisk (*) indicates publications under University of Delaware affiliation; underline indicates advisee as main author.]

Book Chapters

[B1] **N.G. Tsoutsos*** and M. Maniatakos, "Lightweight Fault Tolerance for Secure Aggregation of Homomorphic Data," *Security and Fault Tolerance in Internet of Things*, Springer, 2019

Journal Articles

[J28] L. Folkerts and **N.G. Tsoutsos***, "Tyche: Probabilistic Selection over Encrypted Data for Generative Language Models," *Transactions on Internet Technology*, ACM, 2025

[J27] C. Madamopoulos and **N.G. Tsoutsos***, "3D printer audio and vibration side channel dataset for vulnerability research in additive manufacturing security," *Data in Brief*, Elsevier, 2024

- [J26] [O. Ahmed](#), C. Gouert and **N.G. Tsoutsos***, "PEEV: Parse Encrypt Execute Verify - A Verifiable FHE Framework," Access, IEEE, 2024
- [J25] [R. Shokri](#), C. Gouert and **N.G. Tsoutsos***, "MatchEd: Privacy-Preserving Set Similarity based on MinHash," Transactions on Emerging Topics in Computing, IEEE, 2025
- [J24] [L. Folkerts](#), and **N.G. Tsoutsos***, "FHE-MENNs: Opportunities and Pitfalls for Accelerating Fully Homomorphic Private Inference with Multi-Exit Neural Networks," Journal on Emerging Technologies in Computing Systems, ACM, 2026
- [J23] [C. Gouert](#), and **N.G. Tsoutsos***, "Data Privacy Made Easy: Enhancing Applications with Homomorphic Encryption," Transactions on Design Automation of Electronic Systems, ACM, 2025
- [J22] [C. Gouert](#), D. Mouris and **N.G. Tsoutsos***, "HELM: Navigating Homomorphic Encryption through Gates and Lookup Tables," Transactions on Information Forensics and Security, IEEE, 2025
- [J21] [D. Mouris](#) and **N.G. Tsoutsos***, "Masquerade: Verifiable Multi-Party Aggregation with Secure Multiplicative Commitments," Transactions on Internet Technology, ACM, 2024
- [J20] [C. Gouert](#), D. Mouris and **N.G. Tsoutsos***, "Juliet: A Robust and Configurable Encrypted Processor," Transactions on Computers, IEEE, 2024
- [J19] T. Kaewnukultorn, S. Sepulveda-Mora, R. Broadwater, D. Zhu, **N.G. Tsoutsos*** and S. Hegedus, "Smart PV Inverter Cyberattack Detection using Hardware-in-the-Loop Test Facility," Access, IEEE, 2023
- [J18] [L. Folkerts](#), N. Kater and **N.G. Tsoutsos***, "Coelus: A Universal Search Engine for Digital Manufacturing," Access, IEEE, 2023
- [J17] [C. Gouert](#) and **N.G. Tsoutsos***, "Dirty Metadata: Understanding A Threat to Online Privacy," Security & Privacy, IEEE, 2022
- [J16] [D. Mouris](#) and **N.G. Tsoutsos***, "NFTs For 3D Models: Sustaining Ownership In Industry 4.0," Consumer Electronics Magazine, IEEE, 2022
- [J15] [D. Mouris](#), C. Gouert and **N.G. Tsoutsos***, "Privacy-Preserving IP Verification," Transactions on Computer-Aided Design of Integrated Circuits and Systems, IEEE, 2021
- [J14] [D. Mouris](#) and **N.G. Tsoutsos***, "Zilch: A Framework for Deploying Transparent Zero-Knowledge Proofs," Transactions on Information Forensics and Security, IEEE, 2021
- [J13] [D. Mouris](#), C. Gouert, N. Gupta and **N.G. Tsoutsos***, "Peak your Frequency: Advanced Search of 3D CAD Files in the Fourier Domain," Access, IEEE, 2020
- [J12] W. Li, G. Mac, **N.G. Tsoutsos***, N. Gupta and R. Karri, "Computer aided design (CAD) model search and retrieval using frequency domain file conversion," Additive Manufacturing, Elsevier, 2020
- [J11] **N.G. Tsoutsos***, N. Gupta and R. Karri, "Cybersecurity Road Map for Digital Manufacturing," Computer, IEEE, 2020
- [J10] O. Mazonka, E. Sarkar, E. Chielle, **N.G. Tsoutsos***, and M. Maniatakos, "Practical Data-in-Use Protection Using Binary Decision Diagrams," Access, IEEE, 2020
- [J9] E. Chielle, **N.G. Tsoutsos***, O. Mazonka and M. Maniatakos, "Encrypt-Everything-Everywhere: ISA Extensions for Private Computation," Transactions on Dependable and Secure Computing, IEEE, 2020
- [J8] **N.G. Tsoutsos** and M. Maniatakos, "Efficient Detection for Malicious and Random Errors in Additive Encrypted Computation," Transactions on Computers, IEEE, 2018
- [J7] **N.G. Tsoutsos** and M. Maniatakos, "Anatomy of Memory Corruption Attacks and Mitigations in Embedded Systems," Embedded System Letters, IEEE, 2018

- [J6] D. Mouris, **N.G. Tsoutsos** and M. Maniatakos, "TERMinator Suite: Benchmarking Privacy-Preserving Architectures," Computer Architecture Letters, IEEE, 2018
- [J5] F. Chen, Y. Luo, **N.G. Tsoutsos**, M. Maniatakos, K. Shahin, N. Gupta, "Embedding Tracking Codes in Additive Manufactured Parts for Product Authentication," Advanced Engineering Materials, Wiley, 2018
- [J4] O. Mazonka, **N.G. Tsoutsos** and M. Maniatakos, "Cryptoleq: A Heterogeneous Abstract Machine for Encrypted and Unencrypted Computation," Transactions on Information Forensics and Security, IEEE, 2016
- [J3] S.E. Zeltmann, N. Gupta, **N.G. Tsoutsos**, M. Maniatakos, J. Rajendran and R. Karri, "Manufacturing and Security Challenges in 3D Printing," JOM, Springer, 2016
- [J2] **N.G. Tsoutsos** and M. Maniatakos, "The HEROIC Framework: Encrypted Computation without Shared Keys," Transactions on Computer-Aided Design of Integrated Circuits and Systems, IEEE, 2015
- [J1] **N.G. Tsoutsos** and M. Maniatakos, "Fabrication attacks: Zero-overhead malicious modifications enabling modern microprocessor privilege escalation," Transactions on Emerging Topics in Computing, IEEE, 2014

Conference Papers

- [C32] R. Shokri, and **N.G. Tsoutsos***, "Scytale: A Compiler Framework for Accelerating TFHE with Circuit Bootstrapping," Design, Automation & Test in Europe (DATE), 2026
- [C31] R. Shokri, C. Gouert and **N.G. Tsoutsos***, "HElix: Genome Similarity Detection in the Encrypted Domain," IEEE International Conference on Computer Design (ICCD), 2025 (*Best Paper Award Candidate*)
- [C30] C. Gouert and **N.G. Tsoutsos***, "PolyFHEmus: Rethinking Multiplication in Fully Homomorphic Encryption," IEEE Symposium on VLSI (ISVLSI), 2025
- [C29] R. Shokri, and **N.G. Tsoutsos***, "CHESS: Compiling Homomorphic Encryption with Scheme Switching," IEEE Hardware Oriented Security and Trust (HOST) Symposium, 2025
- [C28] L. Folkerts, and **N.G. Tsoutsos***, "Testing Robustness of Homomorphically Encrypted Split Model LLMs," Design, Automation & Test in Europe (DATE), 2025
- [C27] C. Gouert, M. Ugurbil, D. Mouris, M. de Vega and **N.G. Tsoutsos***, "Ripple: Accelerating Programmable Bootstraps for FHE with Wavelet Approximations," Information Security Conference (ISC), 2024
- [C26] D. Mouris, C. Patton, H. Davis, P. Sarkar and **N.G. Tsoutsos***, "Mastic: Private Weighted Heavy-Hitters and Attribute-Based Metrics," Privacy Enhancing Technologies Symposium (PETS), 2025
- [C25] C. Gouert, V. Joseph, S. Dalton, C. Augonnet, M. Garland and **N.G. Tsoutsos***, "Hardware-Accelerated Encrypted Execution of General-Purpose Applications," Privacy Enhancing Technologies Symposium (PETS), 2025
- [C24] D. Mouris, P. Sarkar and **N.G. Tsoutsos***, "PLASMA: Private, Lightweight Aggregated Statistics against Malicious Adversaries," Privacy Enhancing Technologies Symposium (PETS), 2024
- [C23] D. Mouris, C. Gouert and **N.G. Tsoutsos***, "MPloC: Privacy-Preserving IP Verification using Logic Locking and Secure Multiparty Computation," IEEE Symposium on On-Line Testing (IOLTS), 2023
- [C22] T. White, C. Yang, C. Gouert and **N.G. Tsoutsos***, "FHE-Booster: Accelerating Fully Homomorphic Execution with Fine-tuned Bootstrapping Scheduling," IEEE Hardware Oriented Security and Trust (HOST) Symposium, 2023
- [C21] L. Folkerts, C. Gouert and **N.G. Tsoutsos***, "REDsec: Running Encrypted Discretized Neural Networks in Seconds," Network and Distributed System Security (NDSS) Symposium, 2023
- [C20] C. Gouert, D. Mouris and **N.G. Tsoutsos***, "SoK: New Insights into Fully Homomorphic Encryption Libraries via Standardized Benchmarks," Privacy Enhancing Technologies Symposium (PETS), 2023

- [C19] D. Mouris, C. Gouert and **N.G. Tsoutsos***, "zk-Sherlock: Exposing Hardware Trojans in Zero-Knowledge," IEEE Symposium on VLSI, 2022
- [C18] I. Zografopoulos, C. Konstantinou, **N.G. Tsoutsos***, D. Zhu, and R. Broadwater, "Security assessment and impact analysis of cyberattacks in integrated T&D power systems," IEEE Modeling and Simulation of Cyber-Physical Energy Systems, 2021
- [C17] D. Mouris, **N.G. Tsoutsos***, "Pythia: Intellectual Property Verification in Zero-Knowledge," IEEE/ACM Design Automation Conference, 2020
- [C16] C. Gouert, **N.G. Tsoutsos***, "ROMEO: Conversion and Evaluation of HDL Designs in the Encrypted Domain," IEEE/ACM Design Automation Conference, 2020
- [C15] P. Cronin, C. Gouert, D. Mouris, **N.G. Tsoutsos***, C. Yang, "Covert Data Exfiltration Using Light and Power Channels," IEEE International Conference on Computer Design, 2019
- [C14] M. Nabeel, M. Ashraf, E. Chielle, **N.G. Tsoutsos*** and M. Maniatakos, "CoPHEE: Co-processor for Partially Homomorphic Encrypted Execution," IEEE Hardware Oriented Security and Trust, 2019
- [C13] **N.G. Tsoutsos**, O. Mazonka and M. Maniatakos, "Memory-bounded Randomness for Hardware-constrained Encrypted Computation," IEEE International Conference on Computer Design, 2017
- [C12] **N.G. Tsoutsos** and M. Maniatakos, "Obfuscating Branch Decisions based on Encrypted Data using MISR and Hash Digests," IEEE Asian Hardware Oriented Security and Trust, 2017
- [C11] **N.G. Tsoutsos**, H. Gamil and M. Maniatakos, "Secure 3D Printing: Reconstructing and Validating Solid Geometries Using Toolpath Reverse Engineering," ACM Cyber Physical Systems Security, 2017
- [C10] D. Tychalas, **N.G. Tsoutsos** and M. Maniatakos, "SGXCrypter: IP Protection for Portable Executables using Intel's SGX Technology," Asia and South Pacific Design Automation Conference, 2017
- [C9] N. Gupta, F. Chen, **N.G. Tsoutsos** and M. Maniatakos, "ObfusCADE: Obfuscating Additive Manufacturing CAD Models Against Counterfeiting," IEEE/ACM Design Automation Conference, 2017
- [C8] **N.G. Tsoutsos** and M. Maniatakos, "Cryptographic Vote-Stealing Attacks Against a Partially Homomorphic E-voting Architecture," IEEE International Conference on Computer Design, 2016
- [C7] A. Keliris, C. Konstantinou, **N.G. Tsoutsos**, R. Baiad, and M. Maniatakos, "Enabling Multi-Layer Cyber-Security Assessment of Industrial Control Systems through Hardware-in-the-Loop Testbeds," Asia and South Pacific Design Automation Conference, 2016
- [C6] **N.G. Tsoutsos** and M. Maniatakos, "Extending Residue-based Fault Tolerance to Encrypted Computation," IEEE International Test Conference, 2015
- [C5] **N.G. Tsoutsos** and M. Maniatakos, "Obfuscated arbitrary computation using cryptographic primitives," IEEE Information and Digital Technologies, 2015
- [C4] **N.G. Tsoutsos** and M. Maniatakos, "HEROIC: Homomorphically Encrypted One Instruction Computer," IEEE/EDAA Design Automation and Test in Europe, 2014
- [C3] **N.G. Tsoutsos**, C. Konstantinou and M. Maniatakos, "Advanced Techniques for Designing Stealthy Hardware Trojans," IEEE/ACM Design Automation Conference, 2014
- [C2] **N.G. Tsoutsos** and M. Maniatakos, "Trust no one: Thwarting 'heartbleed' attacks using privacy-preserving computation," IEEE Symposium on VLSI, 2014
- [C1] **N.G. Tsoutsos** and M. Maniatakos, "Investigating the Application of One Instruction Set Computing for Encrypted Data Computation," IACR International Conference on Security, Privacy and Applied Cryptography, 2013

Internet Drafts

[F1] H. Davis, [D. Mouris](#), C. Patton, P. Sarkar and **N.G. Tsoutsos***, "The Mastic VDAF," Available: <https://www.ietf.org/archive/id/draft-mouris-cfrg-mastic-01.html> (authors in alphabetical order, main author D. Mouris)

Technical Reports

[T13] [A. Chakraborty](#) and **N. G. Tsoutsos***, "Privacy-Preserving Federated Inference for Genomic Analysis with Homomorphic Encryption," International Association for Cryptologic Research, Cryptology Archive Report 2025/1515

[T12] [O. Ahmed](#) and **N.G. Tsoutsos***, "PulpFHE: Complex Instruction Set Extensions for FHE Processors," International Association for Cryptologic Research, Cryptology Archive Report 2024/1315

[T11] [C. Gouert](#), M. Ugurbil, D. Mouris, M. de Vega and **N.G. Tsoutsos***, "Ripple: Accelerating Programmable Bootstraps for FHE with Wavelet Approximations," International Association for Cryptologic Research, Cryptology Archive Report 2024/866

[T10] [D. Mouris](#), H. Davis, C. Patton, P. Sarkar and **N.G. Tsoutsos***, "Mastic: Private Weighted Heavy-Hitters and Attribute-Based Metrics," International Association for Cryptologic Research, Cryptology Archive Report 2024/221

[T9] [C. Gouert](#), and **N.G. Tsoutsos***, "Data Privacy Made Easy: Enhancing Applications with Homomorphic Encryption," International Association for Cryptologic Research, Cryptology Archive Report 2024/118

[T8] [C. Gouert](#), D. Mouris, and **N.G. Tsoutsos***, "HELM: Navigating Homomorphic Encryption through Gates and Lookup Tables," International Association for Cryptologic Research, Cryptology Archive Report 2023/1382

[T7] [C. Gouert](#), V. Joseph, S. Dalton, C. Augonnet, M. Garland and **N.G. Tsoutsos***, "Hardware-Accelerated Encrypted Execution of General-Purpose Applications," International Association for Cryptologic Research, Cryptology Archive Report 2023/641

[T6] [D. Mouris](#), P. Sarkar and **N.G. Tsoutsos***, "PLASMA: Private, Lightweight Aggregated Statistics against Malicious Adversaries," International Association for Cryptologic Research, Cryptology Archive Report 2023/080

[T5] [C. Gouert](#), R. Khan and **N.G. Tsoutsos***, "Optimizing Homomorphic Encryption Parameters for Arbitrary Applications," International Association for Cryptologic Research, Cryptology Archive Report 2022/575

[T4] [D. Mouris](#) and **N.G. Tsoutsos***, "Masquerade: Verifiable Multi-Party Aggregation with Secure Multiplicative Commitments," International Association for Cryptologic Research, Cryptology Archive Report 2021/1370

[T3] [L. Folkerts](#), C. Gouert and **N.G. Tsoutsos***, "REDsec: Running Encrypted DNNs in Seconds," International Association for Cryptologic Research, Cryptology Archive Report 2021/1100

[T2] M. Nabeel, M. Ashraf, E. Chielle, **N.G. Tsoutsos*** and M. Maniatakos, "Technical report: CoPHEE: Co-processor for Partially Homomorphic Encrypted Execution," International Association for Cryptologic Research, Cryptology Archive Report 2021/659

[T1] E. Chielle, O. Mazonka, **N.G. Tsoutsos*** and M. Maniatakos, "E³: A Framework for Compiling C++ Programs with Encrypted Operands," International Association for Cryptologic Research, Cryptology Archive Report 2018/1013

Selected Posters

[S1] [D. Mouris](#), P. Sarkar and **N.G. Tsoutsos***, "PLASMA: Private, Lightweight Aggregated Statistics against Malicious Adversaries with Full Security," RSA Conference, 2023

Patents

[P2] **N.G. Tsoutsos**, N. Gupta and M. Maniatakos, "Systems and Methods for Malware Detection in Additive Manufactured Parts," U.S. Patent 11,046,009 B2, 2021

[P1] M. Maniatakos and **N.G. Tsoutsos**, "Homomorphically Encrypted One Instruction Computation Systems and Methods," U.S. Patent 9619658 B2, 2017

Google Scholar profile

Available online: <https://scholar.google.com/citations?user=f3TVR3kAAAAJ> (or <https://tinyurl.com/tsoutsos>).

Source Code Repositories

- [R42] [L. Folkerts](#), R. Shokri, J. Lenis, **N.G. Tsoutsos***, "CSAW Embedded Security Challenge 2025," Available: github.com/TrustworthyComputing/csaw_esc_2025
- [R41] [L. Folkerts](#), R. Shokri, J. Lenis, **N.G. Tsoutsos***, "Microelectronics Security Competition 2025," Available: github.com/TrustworthyComputing/Security_Challenge_2025
- [R40] [R. Shokri](#), **N.G. Tsoutsos***, "CHESS: Compiling Homomorphic Encryption with Scheme Switching," Available: github.com/TrustworthyComputing/CHESS
- [R39] [L. Folkerts](#), **N.G. Tsoutsos***, "GPT-Thief: Testing Robustness of Homomorphically Encrypted Split Model LLMs," Available: github.com/TrustworthyComputing/GPT-thief
- [R38] [O. Ahmed](#), **N.G. Tsoutsos***, "PulpFHE: Complex Instruction Set Extensions for FHE Processors," Available: github.com/TrustworthyComputing/PulpFHE
- [R37] [L. Folkerts](#), R. Shokri, O. Ahmed, **N.G. Tsoutsos***, "CSAW Embedded Security Challenge 2024," Available: github.com/TrustworthyComputing/csaw_esc_2024
- [R36] [C. Gouert](#), **N.G. Tsoutsos***, "The Walrus Library for Parameterizing of Homomorphic Evaluation," Available: github.com/TrustworthyComputing/walrus
- [R35] [D. Mouris](#), C. Patton, **N.G. Tsoutsos***, "Mastic: Private Weighted Heavy-Hitters and Attribute-Based Metrics," Available: github.com/TrustworthyComputing/mastic
- [R34] [R. Shokri](#), C. Gouert, **N.G. Tsoutsos***, "MatchEd: Privacy-Preserving Set Similarity based on MinHash," Available: github.com/TrustworthyComputing/minhash-HE
- [R33] [L. Folkerts](#), **N.G. Tsoutsos***, "FHE-MENNs: Accelerating Fully Homomorphic Private Inference with Multi-Exit Neural Networks," Available: github.com/TrustworthyComputing/FHE-MENN
- [R32] [L. Folkerts](#), **N.G. Tsoutsos***, "Tyche: Probabilistic Selection over Encrypted Data for Generative Language Models," Available: github.com/TrustworthyComputing/Tyche
- [R31] [O. Ahmed](#), C. Gouert, **N.G. Tsoutsos***, "PEEV: Parse Encrypt Execute Verify - A Verifiable FHE Framework," Available: github.com/TrustworthyComputing/PEEV-verifiableFHE
- [R30] [O. Ahmed](#), **N.G. Tsoutsos***, "YAP: Yet Another Parser," Available: github.com/TrustworthyComputing/YAParser
- [R29] [D. Mouris](#), **N.G. Tsoutsos***, "FHE Playgrounds: Get started with Homomorphic Encryption," Available: github.com/TrustworthyComputing/FHE-Playgrounds
- [R28] [J. C. Diaz Vidal](#), **N.G. Tsoutsos***, "FHE IDE: Browser-based Programming Environment for Homomorphic Encryption," Available (by invitation): github.com/TrustworthyComputing/Theia-FHE
- [R27] [C. Gouert](#), D. Mouris, **N.G. Tsoutsos***, "HELM: Navigating Homomorphic Evaluation through Gates and Lookups," Available: github.com/TrustworthyComputing/helm
- [R26] [L. Folkerts](#), C. Gouert, B. Bauer, **N.G. Tsoutsos***, "CSAW Embedded Security Challenge 2023," Available: github.com/TrustworthyComputing/csaw_esc_2023
- [R25] [D. Mouris](#), **N.G. Tsoutsos***, "PLASMA: Private, Lightweight Aggregated Statistics against Malicious Adversaries," Available: github.com/TrustworthyComputing/plasma

- [R24] [C. Gouert](#), D. Mouris, **N.G. Tsoutsos***, "Juliet: A Configurable Processor for Computing on Encrypted Data," Available: github.com/TrustworthyComputing/Juliet
- [R23] [C. Gouert](#), D. Mouris, **N.G. Tsoutsos***, "A Compiler for High-level Java Code to Juliet Homomorphic Assembly," Available: github.com/TrustworthyComputing/HEJava-compiler
- [R22] [C. Gouert](#), D. Mouris, **N.G. Tsoutsos***, "HDL Benchmarks: Verilog designs and their synthesized netlists," Available: github.com/TrustworthyComputing/hdl-benchmarks
- [R21] [D. Mouris](#), C. Gouert, **N.G. Tsoutsos***, "MPloC: Privacy-Preserving IP Verification using Logic Locking and Secure Multiparty Computation," Available: github.com/TrustworthyComputing/mploc
- [R20] [L. Folkerts](#), **N.G. Tsoutsos***, "Coeus: A Universal Search Engine for Additive Manufacturing," Available: github.com/TrustworthyComputing/Coeus
- [R19] [C. Gouert](#), D. Mouris, **N.G. Tsoutsos***, "T2: A cross compiler and standardized benchmarks for FHE computation," Available: github.com/TrustworthyComputing/T2-FHE-Compiler-and-Benchmarks
- [R18] [L. Folkerts](#), C. Gouert, **N.G. Tsoutsos***, "REDsec: Running Encrypted Discretized Neural Networks in Seconds," Available: github.com/TrustworthyComputing/REDsec
- [R17] [C. Gouert](#), D. Mouris, L. Folkerts, **N.G. Tsoutsos***, "CSAW Embedded Security Challenge 2022," Available: github.com/TrustworthyComputing/csaw_esc_2022
- [R16] [C. Gouert](#), **N.G. Tsoutsos***, "(RED)cuFHE: Evolution of FHE acceleration for Multi-GPUs," Available: github.com/TrustworthyComputing/REDcuFHE
- [R15] [D. Mouris](#), **N.G. Tsoutsos***, "Masquerade: Verifiable Multi-Party Aggregation with Secure Multiplicative Commitments," Available (by invitation): github.com/TrustworthyComputing/masquerade
- [R14] [D. Mouris](#), **N.G. Tsoutsos***, "Zilch: A Framework for Deploying Transparent Zero Knowledge Proofs," Available: github.com/TrustworthyComputing/Zilch
- [R13] [D. Mouris](#), **N.G. Tsoutsos***, "ZeroJava to zMIPS compiler," Available: github.com/TrustworthyComputing/ZeroJava-compiler
- [R12] [D. Mouris](#), **N.G. Tsoutsos***, "Pythia: Intellectual Property Verification in Zero-Knowledge," Available (by invitation): github.com/TrustworthyComputing/Pythia
- [R11] [C. Gouert](#), D. Mouris, L. Folkerts, **N.G. Tsoutsos***, "CSAW Embedded Security Challenge 2021," Available: github.com/TrustworthyComputing/csaw_esc_2021
- [R10] [D. Mouris](#), C. Gouert, **N.G. Tsoutsos***, "Fourier-Fingerprint-Search: Advanced Search of 3D CAD Files in the Fourier Domain," Available: github.com/TrustworthyComputing/Fourier-Fingerprint-Search
- [R9] [C. Gouert](#), **N.G. Tsoutsos***, "Romeo: A framework for translating Verilog program to fully homomorphic circuits," Available: github.com/TrustworthyComputing/Romeo
- [R8] [C. Gouert](#), D. Mouris, L. Folkerts, **N.G. Tsoutsos***, "CSAW Embedded Security Challenge 2020," Available: github.com/TrustworthyComputing/csaw_esc_2020
- [R7] P. Cronin, C. Gouert, **N.G. Tsoutsos***, "CSAW Embedded Security Challenge 2019," Available: github.com/TrustworthyComputing/csaw_esc_2019
- [R6] D. Mouris, **N.G. Tsoutsos**, M. Maniatakos, "TERMinator Suite: A collection of benchmarks for privacy-preserving architectures," Available: github.com/momalab/TERMinatorSuite
- [R5] D. Tychalas, **N.G. Tsoutsos**, M. Maniatakos, "SGXCrypter: A crypter for IP Protection of Windows Portable Executables using Intel's Software Guard Extensions," Available: github.com/momalab/SGXCrypter

[R4] O. Mazonka, **N.G. Tsoutsos**, M. Maniatakos, "Cryptoleq: A compiler and abstract machine emulator for encrypted and unencrypted computation," Available: github.com/momalab/cryptoleq

[R3] A. Keliris, **N.G. Tsoutsos**, M. Maniatakos "CSAW Embedded Security Challenge 2017," Available: github.com/momalab/csaw_esc_2017

[R2] **N.G. Tsoutsos**, "CSAW Embedded Security Challenge 2016," Available: github.com/nekt/csaw_esc_2016

[R1] **N.G. Tsoutsos**, "CSAW Embedded Security Challenge 2015," Available: github.com/nekt/csaw_esc_2015

Open-Access Tutorials

[W1] D. Mouris, **N.G. Tsoutsos***, "Transparent Zero-Knowledge Proofs With Zilch," Medium.com, 2021

Selected Media Coverage

- Tabitha Groh, "Demystifying Microelectronics," University of Delaware UDaily
Available: <https://www.udel.edu/udaily/2026/february/microelectronics-community-outreach/>
- UD Engineering, "Stronger by Design," University of Delaware UDaily
Available: <https://www.udel.edu/udaily/2025/november/building-stronger-chips-satwik-patnaik/>
- Lois Anne DeLong, "Forever CSAW: Why These Former Competitors Are Still All In," NYU CyberByte
Available: https://issuu.com/nyutandon/docs/cyberbyte_-_spring_2025
- Jamie Washington, "Call for FinTech Papers," University of Delaware UDaily
Available: <https://www.udel.edu/udaily/2024/december/fintech-call-papers-2025-conference/>
- Beth Miller, "New directors for UD's growing fintech endeavors," University of Delaware UDaily
Available: <https://www.udel.edu/udaily/2024/august/fintech-innovation-nektarios-tsoutsos-gang-wang/>
- Erica Brockmeier, "Supporting Cybersecurity Scholars," University of Delaware UDaily
Available: <https://www.udel.edu/udaily/2024/february/cybersecurity-national-science-foundation-scholarships-service-career-placement/>
- Erica Brockmeier, "Improving Cybersecurity," University of Delaware UDaily
Available: <https://www.udel.edu/udaily/2023/july/nektarios-tsoutsos-national-science-foundation-career-cybersecurity-privacy-cloud-computing/>
- Brandon Holveck, "Business: Delaware's most influential people," Delaware News Journal
Available: <https://www.delawareonline.com/in-depth/news/2023/03/21/meet-most-influential-business-leaders-delaware-2023/69823426007/>
- Maddy Lauria, "Encouraging Equity in FinTech," University of Delaware UDaily
Available: <https://www.udel.edu/udaily/2023/january/fintech-innovation-engineering-mobileid/>
- Maddy Lauria, "Degree of the future – Cybersecurity Engineering," University of Delaware Magazine, Volume 30, Number 3, Available: <https://www1.udel.edu/ocm/magazine/UDMagazineV30n3/mobile/index.html>
- Maddy Lauria, "Blue Hens Capture the Flag," University of Delaware UDaily
Available: <https://www.udel.edu/udaily/2022/november/capture-flag-cybersecurity-content-engineering-computer-science/>
- Maddy Lauria, "Degree of the Future," University of Delaware UDaily
Available: <https://www.udel.edu/udaily/2022/june/new-cybersecurity-engineering-degree-2022/>
- UD Engineering, "Blue Hens Capture the Flag," University of Delaware UDaily
Available: <https://www.udel.edu/udaily/2021/april/blue-hens-capture-the-flag-cybersecurity-competition/>
- Julie Stewart, "Training Ethical Hackers," University of Delaware UDaily
Available: <https://www.udel.edu/udaily/2019/april/computer-engineering-student-competitions/>

- UD Engineering, "Team secures NSF grant to advance novel CAD technology for 3D printing," UD ECE News Available: <http://www.ece.udel.edu/2019/2019/team-secures-nsf-grant-to-advance-novel-cad-technology-for-3d-printing/>
- Alessandro Di Fiore, "3D Printing Gives Hackers Entirely New Ways to Wreak Havoc," Harvard Business Review Available: <https://hbr.org/2017/10/3d-printing-gives-hackers-entirely-new-ways-to-wreak-havoc>
- Michael Kassner, "3D Printing Security Risk Caused by Undetectable Defects, and Ways to Prevent It," TechRepublic Available: <https://www.techrepublic.com/article/3d-printing-security-risk-caused-by-undetectable-defects/>
- Pierluigi Paganini, "Fabrication-time Attacks and the Manchurian Chip," Security Affairs Available: <https://securityaffairs.co/wordpress/48141/security/fabrication-time-attacks.html>
- Beau Jackson, "NYU Team Encode Parts with 3D Printed QR 'Clouds' to Prevent Counterfeiting," 3D Printing Industry Available: <https://3dprintingindustry.com/news/nyu-team-encode-parts-with-3d-printed-qr-clouds-to-prevent-counterfeiting-138453/>
- Clare Scott, "Medical and Aerospace 3D Printed Parts Could Be Secured by Embedded QR Codes," 3Dprint.com Available: <https://3dprint.com/223083/3d-printed-embedded-qr-codes/>
- NYU Engineering, "World's Biggest Student-Led Cybersecurity Games Announce Winners of CSAW," Business Insider Available: <https://tinyurl.com/csaw-2018-winners>