Nektarios Georgios Tsoutsos

Assistant Professor, University of Delaware
E-mail: tsoutsos@udel.edu • web: udel.edu/~tsoutsos

Research Interests

- Cybersecurity, Applied Cryptography, Privacy Outsourcing, Hardware Security, Trustworthy Computing, Computer Architecture, Cyberphysical 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

Professional Positions

- **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 –
- **Post-Doctoral Associate**, New York University 01/18 – 08/18
- **Research Assistant**, New York University 01/13 – 01/18
- **Graduate Technical Intern**, Security Center of Excellence, Intel Corporation, Hillsboro, OR 05/14 – 11/14
- **Information Security Advisor**, Obrela Security Industries, Athens, Greece 09/10 – 12/12

Grants

- **Principal Investigator:** *[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), **Current status:** Awarded
- **Principal Investigator:** *[DE-EE0008768-006] Faster-than-real-time Simulation with Demonstration for Resilient DER Integration* 11/19 – 10/22
  Sponsor: Department of Energy (DoE), **Budget: $128k** (UD share), **Current status:** Awarded
- **Co-Principal Investigator:** Cybersecurity Certificate Program 02/21 – 02/23
  Sponsor: JPMorgan Chase, **Budget: $225k**, **Current status:** Awarded
- **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**, **Current status:** Awarded

Professional Service

- **Technical Program Committee: DAC** '20-'21 (track: Hardware Security II: Attack and Defense), **DSN** '20, **ISVLSI** '19-'20-'21 (track: *System Design and Security*), **CPSIoTSec** '20-'21, **CIMSS** '21, **ICCD** '21 (track: Test, Verification, and Security), **ICCD** '19 (track: Processor Architecture), **VLSI-SoC** '19 (track: *Hardware Security*), **AsianHOST** ('19, '20), **VLSI-SoC** '18 (track: *Hardware Security*).
- **External Review Committee: MICRO** '20-'21.
- **Organizing Committee: ICCD** '19
- **General co-chair: R2DM Workshop** '21
- **Technical Referee:** *IEEE* **CAL** ('20), **TMC** ('20), **TCAD** ('20, '19, '18), **TC** ('20), **CEMAG** ('21), **Computer** ('19), **Access** ('19), **ICCD** ('19), **ESL** ('19, '18), **TIFS** ('19, '17, '16), **TETC** ('19, '18, '17), **AsianHOST** ('19), , **MICRO** ('19), **ISIT** ('19), **ISVLSI** ('19, '18), **VTS** ('18), **ITC** ('18, '17), **VLSI-SoC** ('19), **D&T** ('16); *ACM* **TODAES** ('16, '15); *Springer* **JCEN** ('20), **AIHC** ('20, '19), **JETT** ('19), **HASS** ('17), **SCIS** ('16); *MDPI* **Cryptography** ('20); *Elsevier* **DSP** ('17), **ADDMA** ('17), **JISA** ('16); *IET* **ELL** ('17); *Euromicro* **DSD** ('16).
- **Technical Sub-reviewer**: *IEEE/ACM* **DAC** ('16, '15, '14), **ICCAD** ('15, '16); *IEEE* **HOST** ('20), **DSN** ('21), **ASPDAC** ('18), **TIFS** ('15, '14, '13), **TComp** ('19, '16), **TETC** ('13), **TCAD** ('19, '14), **ITC** ('18, '15, '14), **VTS** ('17), **ETS** ('18), **ISVLSI** ('16, '15, '14),

ICCD ('13), **AsianHOST** ('17), **IOLTS** ('17, '16), **DTIS** ('16, '14); *ACM* **AsiaCCS** ('18, '17), **TECS** ('14), **GLSVLSI** ('16), **CPS-SPC** ('15), **CASES** ('16, '15); *Elsevier* **FGCS** ('15).

- **Session Chair/Moderator: DATE** '21 (session: Attacks and defense mechanisms), **ICCAD** '20 (session: Top Picks in Hardware and Embedded Security), **DAC** '19 (session: *Leaking like a Sieve: Exploits and Mitigations for Architecture Side Channels*), **HOST** '19 (session: *(Anti)Reverse Engineering and Obfuscation*), **ICCAD** '18 (sessions: *Designing and Assessing Secure Architectures*, *Approximate Computing*), **ICCD** '17 (session: *Synthesis and Security*)

University Service

- **Faculty Search Committee:** ECE Department, University of Delaware 09/18 – 07/19
- **Graduate Committee:** ECE Department, University of Delaware 09/18 –
- **Cybersecurity Steering Committee:** ECE Department, University of Delaware 09/19 –

Community Service

- **Challenge Leader/Organizer:** Embedded Systems Challenge, Cyber Security Awareness Worldwide 06/15 – 11/17
- **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 –

Teaching

- **University of Delaware, ECE Department**

CPEG 475/675 - IoT and Embedded Systems Security	Spring 2019
CPEG 475/675 - IoT and Embedded Systems Security	Fall 2019
CPEG 472/672 - Applied Cryptography	Spring 2020
CPEG 475/675 - IoT and Embedded Systems Security	Fall 2020
CPEG 472/672 - Applied Cryptography	Spring 2021
CPEG 697 - Advanced Cybersecurity	Fall 2021
CPEG 475/675 - IoT and Embedded Systems Security	Fall 2021

Advisees and Interns

- **Charles Gouert**, Ph.D. student – University of Delaware, Trustworthy Computing Group 09/18 –
- **Dimitris Mouris**, Ph.D. student – University of Delaware, Trustworthy Computing Group 01/19 –
- **Lars Folkerts**, Ph.D. student – University of Delaware, Trustworthy Computing Group 06/20 –
- **Manish Chaudhary**, M.Sc. student – University of Delaware, Trustworthy Computing Group 09/19 –
- **Nicholas Kater**, Undergraduate student – University of Delaware, Trustworthy Computing Group 07/20 – 08/21
- **Maggie McGrath**, Undergraduate student – University of Delaware, Trustworthy Computing Group 01/19 – 02/19
- **Ryan Peterson**, Undergraduate student – University of Delaware, Trustworthy Computing Group 07/19 – 08/19
- **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

- **New York University Ph.D. Student Fellowship** 01/13 – 12/17
- **Pearl Brownstein Doctoral Research Award** for doctoral research showing the greatest promise (NYU) 05/18
- **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 11/18

- **Advisee Honor: 3rd Place Award** at CSAW Hack3D for reverse engineering additive manufacturing files 11/20
- **Advisee Honor: 1st Place Award** at ECE Research Day for privacy-preserving neural network inference 05/21
- **Advisee Honor: Graduate Faculty Award** on Computer Systems & Networks 05/21

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

[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. Goupta 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 *(January 2018 spotlight paper)*

[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 *(Most-read engineering paper of 2016 at Springer Publishing)*

[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 Proceedings

[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 MSCPES 2021

[C17] D. Mouris, **N. G. Tsoutsos**, "Pythia: Intellectual Property Verification in Zero-Knowledge," ACM/EDAC/IEEE DAC 2020

[C16] C. Gouert, **N.G. Tsoutsos**, "ROMEO: Conversion and Evaluation of HDL Designs in the Encrypted Domain," ACM/EDAC/IEEE DAC 2020

[C15] P. Cronin, C. Gouert, D. Mouris, **N.G. Tsoutsos**, C. Yang, "Covert Data Exfiltration Using Light and Power Channels," IEEE ICCD 2019

[C14] M. Nabeel, M. Ashraf, E. Chielle, **N.G. Tsoutsos** and M. Maniatakos, "CoPHEE: Co-processor for Partially Homomorphic Encrypted Execution," IEEE HOST 2019

[C13] **N.G. Tsoutsos**, O. Mazonka and M. Maniatakos, "Memory-bounded Randomness for Hardware-constrained Encrypted Computation," IEEE ICCD 2017

[C12] **N.G. Tsoutsos** and M. Maniatakos, "Obfuscating Branch Decisions based on Encrypted Data using MISR and Hash Digests," IEEE AsianHOST 2017

[C11] **N.G. Tsoutsos**, H. Gamil and M. Maniatakos, "Secure 3D Printing: Reconstructing and Validating Solid Geometries Using Toolpath Reverse Engineering," ACM CPSS 2017

[C10] D. Tychalas, **N.G. Tsoutsos** and M. Maniatakos, "SGXCrypter: IP Protection for Portable Executables using Intel's SGX Technology," ASPDAC 2017

[C9] N. Gupta, F. Chen, **N.G. Tsoutsos** and M. Maniatakos, "ObfusCADe: Obfuscating Additive Manufacturing CAD Models Against Counterfeiting," ACM/EDAC/IEEE DAC 2017

[C8] **N.G. Tsoutsos** and M. Maniatakos, "Cryptographic Vote-Stealing Attacks Against a Partially Homomorphic E-voting Architecture," IEEE ICCD 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," ASPDAC 2016

[C6] **N.G. Tsoutsos** and M. Maniatakos, "Extending Residue-based Fault Tolerance to Encrypted Computation," IEEE ITC 2015

[C5] **N.G. Tsoutsos** and M. Maniatakos, "Obfuscated arbitrary computation using cryptographic primitives," IEEE IDT 2015

[C4] **N.G. Tsoutsos** and M. Maniatakos, "HEROIC: Homomorphically EncRypted One Instruction Computer," DATE 2014

[C3] **N.G. Tsoutsos**, C. Konstantinou and M. Maniatakos, "Advanced Techniques for Designing Stealthy Hardware Trojans," ACM/EDAC/IEEE DAC 2014

[C2] **N.G. Tsoutsos** and M. Maniatakos, "Trust no one: Thwarting 'heartbleed' attacks using privacy-preserving computation," IEEE ISVLSI 2014

[C1] **N.G. Tsoutsos** and M. Maniatakos, "Investigating the Application of One Instruction Set Computing for Encrypted Data Computation," IACR SPACE 2013

Technical Reports

[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] E. Chielle, O. Mazonka, **N.G. Tsoutsos** and M. Maniatakos, "E^3: A Framework for Compiling C++ Programs with Encrypted Operands," International Association for Cryptologic Research, Cryptology Archive Report 2018/1013

[T1] M. Nabeel, M. Ashraf, E. Chielle, **N.G. Tsoutsos** and M. Maniatakos, "Technical report: CoPHEE: Co-processor for Partially Homomorphic Encrypted Execution," Available: https://tinyurl.com/CoPHEE-techreport

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

Open-Source Repositories

[R12] D. Mouris, **N.G. Tsoutsos**, "Zilch: A Framework for Deploying Transparent Zero Knowledge Proofs," Available: github.com/TrustworthyComputing/Zilch

[R10] D. Mouris, **N.G. Tsoutsos**, "ZeroJava to zMIPS compiler," Available: github.com/TrustworthyComputing/ZeroJAva-compiler

[R10] C. Gouert, D. Mouris, L. Folkerts, **N.G. Tsoutsos**, "CSAW Embedded Security Challenge 2021," Available: github.com/TrustworthyComputing/csaw_esc_2021

[R9] 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

[R8] C. Gouert, **N.G. Tsoutsos**, "Romeo: A framework for translating Verilog program to fully homomorphic circuits," Available: github.com/TrustworthyComputing/Romeo

[R7] 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

Select Media Coverage

- 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