IOANNIS "YANNIS" ROUSELAKIS

yannis@rouselakis.com

Education

- **The University of Texas at Austin**
  Ph. D., Computer Science, Jan. 2008 – Aug. 2013 GPA 3.96 / 4
  Advisor: *Brent Waters*
  Dissertation: *Attribute-Based Encryption: Robust and Efficient Constructions*
- **The National Technical University of Athens**
  B. E. (Diploma), School of Electrical and Computer Engineering, Sept. 2002 – Dec. 2007 Grade 9.74 / 10
  Advisor: *Stathis Zachos*
  Diploma Thesis: *Translation from Quantum Programming Language nQml to Quantum Circuits.*

Work Experience

- **Senior Cryptographic Developer in NTT Research, London (Feb. 2022 - Present):** Working under the management of Kei Karasawa (until mid-2023) and Takashi Goto in the Technology Promotion group. Primary focus revolves around promoting and deploying Attribute-Based Encryption solutions as well as maintaining, improving, and developing the NTK advanced-crypto library.
  Employer: Takashi Goto, Technology Promotion – NTT Research.
- **Senior Java Developer in Wise Inc., London (Nov. 2020 – Feb. 2022):** Working under the management of Frane Roje in the Risk Management – Treasury team. I explored, implemented, and improved various risk analysis algorithms for several Wise financial products.
  Employer: Frane Roje, Risk Management – Treasury.
- **Software Developer in Google, Redmond (Apr. 2018 – Apr. 2019):** Working under the management of Hany Farag in the Production Security (ProdSec) group on the Unified Certificate Authority (CA) and the Google Cloud Managed CA.
  Employer: Hany Farag, ProdSec – Google Cloud.
- **Software Developer in Microsoft, Redmond (Sep. 2013 – Apr. 2018):** Working under the management of Xiaohong Su in the Windows Cryptography product group on the various cryptographic libraries of Windows OS and the Data Protection API (DPAPI).
  Employer: Xiaohong Su, Windows Core – OSG – Trust Management group
- **Summer Internship in Microsoft, Redmond (Jun. 2013 – Aug. 2013):** Worked under the supervisor of Nathan Ide and the guidance of my coach Saurav Sinha to implement a new feature on the Windows Login functionality.
  Employer: Nathan Ide, Windows Core – SID – AP group
- **Summer Internship in Microsoft, Redmond (Jun. 2012 – Aug. 2012):** Worked under the supervisor of Irina Gorbach to implement a new feature of the Trust Services Framework. In collaboration with Tom Roeder (MSR), we incorporated the functionality of the CS2 searchable encryption project, designed by the XCG Security and Cryptography group, to TFS.
  Employer: Irina Gorbach, SQL Azure group

- **Summer Internship in Microsoft, Redmond (Jun. 2011 – Aug. 2011):** Worked under the supervisor of Roy D'Souza and Omkant Pandey towards researching certain cryptographic primitives, which are applicable to certain SQL Azure applications.

  Employer: Roy D'Souza, SQL Azure group

Research Interests

Applied cryptography and network security. Other research interests include complexity theory, artificial intelligence, and quantum computing.

Publications

Deterministic Public-key Encryption under Continual Leakage,
By Venkata Koppula, Omkant Pandey, Yannis Rouselakis, Brent Waters,
In Applied Cryptography and Network Security (ACNS) 2016.

Efficient Statically-Secure Large-Universe Multi-Authority Attribute-Based Encryption,
By Yannis Rouselakis, Brent Waters,
In Financial Cryptography and Data Security 2015.

Practical Constructions and New Proof Methods for Large Universe Attribute-Based Encryption,
By Yannis Rouselakis, Brent Waters,
In ACM Conference on Computer and Communications Security 2013.

Compilation to Quantum Circuits for a Language with Quantum Data and Control,
By Yannis Rouselakis, Nikolaos S. Papaspyrou, Yiannis Tsiouris, Eneia N. Todoran,
In FedCSIS 2013.

Property Preserving Symmetric Encryption,
By Omkant Pandey, Yannis Rouselakis, In EUROCRYPT 2012.

Achieving Leakage Resilience through Dual System Encryption,
By Allison Lewko, Yannis Rouselakis, Brent Waters, In TCC 2011.

Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions,
By Sherman Chow, Yevgeniy Dodis, Yannis Rouselakis, Brent Waters,
In ACM Conference on Computer and Communications Security 2010: 152-16

Honors and Awards

- Fellowship from the Greek National Scholarship Institute (I.K.Y.) for the 1st , 2nd, and 3rd years of undergraduate studies for being among the top 5 students.
- Papakyriakopoylos Award for the academic year 2003-2004 (top grades in 5 math courses).
- MCD Fellowship from the University of Texas at Austin.

Undergraduate Research Experience

- Investigated efficient ways to translate quantum programming commands to quantum circuits. Wrote a Haskell application that produces the circuit of any algorithm written in nQml. [NTU Athens]
- Implemented in C++ an artificial intelligence program that used heuristic algorithms to solve the marble solitaire game of arbitrary size. [NTU Athens]

Skills

- Programming — C, Assembly (x86, ARM), C++, C#, Java, Haskell, JavaScript, Prolog, SQL
- Applications — Visual Studio, Eclipse, Matlab, Mathematica, AutoCAD, Photoshop CS
- Databases — MySQL, Oracle, MS-Access
- Languages — Greek (Native), English (Fluent), German (Beginner)