Exponent®
Engineering & Scientific Consulting

Riley Vaughn, Ph.D.
Scientist | Computer, Data & Security Sciences
Irvine
+1-949-242-6079 | rvaughn@exponent.com

Professional Profile

Dr. Vaughn is a scientist at Exponent with expertise in computer science, cryptography, cryptanalysis, cybersecurity, and blockchain.

He works on practical and theoretical cryptographic problems, with experience in post-quantum cryptography, algorithmic analysis, scientific programming, secure computational methods, and technical consulting. His work combines technical depth with practical problem solving for complex computational and security-related challenges.

Riley's research and computational analysis include post-quantum cryptographic constructions, cryptographic compression functions, diffusion analysis, secure computing concepts, and algorithmic performance evaluation. His experience also includes software prototyping, machine-learning-based research and technical communication for multidisciplinary projects that require rigorous analytical methods and clear presentation of technical findings.

He addresses technical questions involving cryptographic design and evaluation, computational efficiency, software implementation, data analysis, and mathematically grounded problem solving. His background is particularly relevant to matters involving secure systems, algorithmic performance, analytical modeling, and the interpretation of complex technical information in a clear and defensible manner.

Dr. Vaughn's approach integrates mathematical analysis, software development, computational experimentation, and research-based reasoning to evaluate technical problems from both theoretical and applied perspectives. He has developed analytical workflows, taught undergraduate computer science laboratory sections, and contributed to research in cryptography, cryptanalysis, and machine learning. Before joining Exponent, he held graduate level research and teaching roles at the University of Wyoming as well as software engineering and research roles at Erie Insurance Group and Brookhaven National Laboratory.

Academic Credentials & Professional Honors

Ph.D., Computer Science, University of Wyoming, 2026

B.S., Computer Science, Edinboro University, 2021

Publications

Vaughn R, Borowczak M. "Relaxation of Strict Avalanche Criterion on All SHA-256 Sub-Function Combinations." Cryptography. 2026.

© 2026 Exponent, Inc. All Rights Reserved

Vaughn R, Borowczak M. "MiNTT: A Family of Module Lattice-Based Cryptographic Compression Functions." IEEE Access. 2026.

Vaughn R, Borowczak M. "Strict avalanche criterion of SHA-256 and sub-function-removed variants." Cryptography. 2024.

Talukder S, Vaughn R. "A template for alternative proof of work for cryptocurrencies." International Conference on Smart Generation Computing, Communication and Networking. 2021.

Vaughn R, Talukder S. "A template for useful proof of work." Journal of Computing Sciences in Colleges. 2020.

Vaughn R. An Analysis of Hash and Compression Functions in Classical and Post-Quantum Settings.

Additional Education & Training

Programming languages: C++, Go, Python, Java, C, C#, R, JavaScript, HTML/CSS, Bash, SQL

Additional technical experience: version control with Git, Linux- and Windows-based workflows, object-oriented design, functional programming