# WANG, SHUANGBAO (PAUL)

Dr. Paul Wang is a Professor and Chair of the Department of Computer Science at Morgan State University. He was a TSYS Endowed Chair in Cybersecurity at Columbus State University and the Director of Center for Security Studies at University of Maryland, University College. Paul was previously Chief Information and Technology Officer (CIO/CTO) of the National Biomedical Research Foundation (NBRF). He has held professorships at many universities including University of Maryland, George Washington University, George Mason University, Columbus State University, Morgan State University, and two other universities. Paul was directly involved in drafting of the National Initiatives of Cybersecurity Education (NICE) framework and is currently a member of the NICE committee. His research areas are secure architecture, IoT/CPS, cryptography, quantum cryptology, and video indexing.

Paul has extensive knowledge and experiences both in theory and practice. He has been speakers to major national cybersecurity conferences. Dr. Wang has been constantly leading the effort in conducting cutting edge research and establishing cybersecurity programs to train military personnel and veterans in the nation and around the world, a $250 million award from U.S. Department of Defense, and Director of the biggest cybersecurity education program in the nation with more than 3,000 graduate cyber students.

In addition to books, refereed publications, conference speakers and numeral grant activities including recent grants from National Security Agency, Paul has four patents; three of them have been licensed to the industry. Dr. Wang became a doctoral candidate at Tsinghua University in 1999 and completed his doctoral dissertation under the guidance of Dr. Robert Ledley, the inventor of the body CT scanner at Georgetown University and received his Ph.D. degree at George Mason University in 2004.

**Abstract:**

**Optimize Quantum Circuits for Fast Cryptanalyzing Pre and Post Quantum Cryptographies**

Most quantum cryptanalytic programs can only break one number (e.g. 15 or 21) at a time due to the fact that each Quantum Fourier Transform (QFT) used to find out a period of a particular prime number, requires a unique quantum circuit. To break the RSA, one needs to design a quantum circuit for each prime number being exploited. Since there are a great amount of prime numbers, the current one by one factor finding approach is apparently not conceivable to put into practical use. This session introduces the most recent research to automatically create quantum circuits and use one program to factor multiple prime numbers. The proposed approach to exploit multiple prime numbers at once is a breakthrough toward actual breaking the RSA algorithm. The results are expected to lead a better understanding of quantum algorithms, optimization, programming, and shorten the time to the success in cryptanalytic tasks.