Abstract:
Computation outsourcing is an integral part of cloud computing. It enables end-users to outsource their computational tasks to the cloud and utilize the shared cloud resources in a pay-per-use manner. However, once the tasks are outsourced, the end-users will lose control of their data, which may result in severe security issues especially when the data is sensitive. To address this problem, secure outsourcing mechanisms have been proposed to ensure security of the end-users’ outsourced data. In our research, we investigate outsourcing of general computational problems that constitute the mathematical basics for problems emerged from various fields such as engineering and finance. In this talk, I will discuss two of our most recent research on computation outsourcing: (i) We propose an affine mapping based Cost-Aware Secure Outsourcing (CASO) scheme. Security analysis demonstrates that CASO can ensure that the cloud is unable to learn any key information from the transformed problem. We also propose a verification scheme to ensure that the end-users will always receive a valid solution from the cloud. (ii) To address the problem of secure outsourcing of modular exponentiation to one single untrusted server, we propose a CryptSOS scheme that can be applied to many cryptographic computations. CryptSOS imposes very limited number of modular multiplications at local environment thus achieving impressive computational gains. CryptSOS also provides a secure verification scheme to ensure that the end-users can always receive valid results.

Bio:
Jian Ren received the BS and MS degrees both in mathematics from Shaanxi Normal University, and received the Ph.D. degree in EE from Xidian University, China. He is an Associate Professor in the Department of ECE at Michigan State University. His current research interests include cryptography, network security, energy efficient sensor network security protocol design, privacy-preserving communications, secure and efficient cloud computing, and cognitive networks. He is a recipient of the US National Science Foundation Faculty Early Career Development (CAREER) award in 2009. Dr. Ren is a senior member of the IEEE.