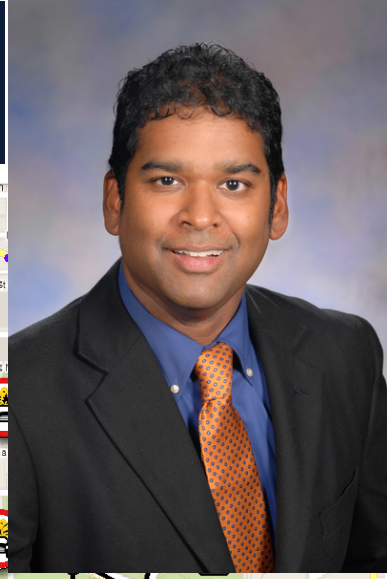
Kevin Butler



Research Objectives and Key Challenges:

- How to ensure private communication in the
- How to achieve exploration and exploitation concurrently
- How to ensure network function in opportunistic networks with adversarial agents with data intermittency

Significance of Work:

- Secure outsourced and amortized garbled circuit computation for efficient multiparty computation
- Hybrid secure computation with secure enclaves to parameterize security and performance (up to 38X performance improvement)

High-Level Technical Approach:

- Secure multiparty computation using garbled circuits
- Cryptographic primitives for efficient communication
- Techniques for leveraging trusted hardware in conjunction with cryptography for efficient private computing

Potential AFRL Collaboration Areas:

- Control systems
- Navigation systems in the face of private/adversarial data

Center Research Areas:

- Security and Privacy of Computed and Stored Data

Recent Accomplishments:

- ✓ Developed compilers for secure computation and partially garbled circuit structures for amortizing computation across execution instances
- ✓ Developed secure one-time program computation using trusted hardware and garbled circuits
- ✓ Developed privacy-preserving localization using secure enclaves

Current Funding:

- NSF, DARPA, ITU, and industry partners

Short-Term Research Vision:

- Incorporating mobile/embedded trustworthy hardware into privacy-preserving localization techniques
- Furthering performance and usability of multiparty computation

UF UNIVERSITY of FLORIDA · Duke UNIVERSITY · TEXAS The University of Texas at Austin · UC SANTA CRUZ