Optimizing Cryptographic Routing

Moving data across a cryptographic network may entail dealing with numerous cryptographic protocols. This talk explores finding quickest paths in cryptographic networks using both commutative and non-commutative symmetric or asymmetric encryption. The cryptographic protocols may add delays to the network links. Hence, this talk models cryptographic data transmission on heterogeneous networks ranging from large client/server machines down to constrained sensors using the quickest path problem for labeled and weighted digraphs. The quickest path problem allows us to model cryptographic costs along with different available network bandwidths. This model assumes the network may be expressed as a directed graph with $n$ nodes whose edges are labeled with terminals from a Dyck or semi-Dyck language. Thus, in these labeled and weighted graphs, a path $P$ is constrained by requiring the list of edge labels along the path $P$ to form a string that is a member of a given Dyck or semi-Dyck language.

Dr. Phillip G. Bradford
Assistant Professor
Department of Computer Science
The University of Alabama