Abstract Given a cryptographic algorithm, it's not evident from inspection how much security it provides. Instead, algorithms are typically evaluated by expert opinion, "the test of time" or, more recently, by security proofs showing that breaking some algorithm reduces to solving some other well-studied problem. This talk will survey how proof techniques are used in cryptography, and examine how these techniques have yielded practical, deployed results. In particular, security proofs are important for evaluating new algorithms for new standards and applications. We will examine the security proofs used in OEAP, pairing-based cryptography, and FFX, a new mode for encryption under consideration by NIST.

Bio Terence Spies has over 19 years of security and systems software development experience, working with leading companies such as Microsoft, Asta Networks and others. Terence now serves as Chief Technology Officer at Voltage Security, overseeing the expansion of Voltage technology into new application areas such as mobility, payments and other areas where application data security is required. Prior to joining Voltage, Terence worked at Asta Networks as Director of Development and VP of Engineering. Before Asta, Terence was with Microsoft for almost 9 years where he started the public key cryptography group and led the development of Microsoft Crypto API. While at Microsoft, Terence also designed the SSL server and client side implementations for Microsoft Internet Explorer, participated in the PCT/TLS protocol design, led the development team for the Microsoft Certificate Server and led the integration of the certificate server and active directory. Terence is active within the standards community and currently serves as chair of X9F1, the Cryptographic Tools group of X9 whose charter is to draft cryptographic algorithm standards for use in the financial industry. Terence graduated with a Bachelor of Science degree in Logic and Computation from Carnegie Mellon University.