1125-B1-213 **Scott C. Batson*** (scott.batson@navy.mil), **Hemant Pendharkar**, **Tuwaner Hudson Lamar**, **Georgianna L.T. Campbell** and **Kayla A. Capitan**. *The Suitability of Lattices for Project-based Introductions to Cryptology.*

Through the completion of common prerequisite courses, the majority of undergraduate students have been exposed to the mathematical concepts necessary to characterize lattices, which may be conceptualized as an arrangement of points in geometric space. Yet, there are also perspectives of lattices that may only be expressed with knowledge of advanced Algebraic Number Theory and Abstract Algebra. While lattice-based cryptography is studied as a strong candidate for post-quantum cryptography, the various aspects of lattices, from simple to complex, are capable of supporting introductions to cryptology at different levels. We first introduce lattices as a topic for cryptologic study. We then identify problems and mathematical aspects of lattice-based cryptography that are interesting and accessible to undergraduate students, graduate students, and/or faculty. Finally, results and outcomes of a lattice-based cryptography research project, with contributions ranging from those of a high school student to terminal degree holders, are discussed. This research experience is presented as an innovative model for project-based introductions to cryptology. (Received August 12, 2016)