1100-94-269 **Ruben Rivera*** (ruben_m_rivera@nnmc.edu), **John Auxier**, **Ajit Hira**, **Susan Nsaba** and **Danelle Jaramillo**. *A Variant on Hashed-MQV Approach to Diffie Hellman Protocol.*

We present some results of our research on cryptography by delineating aspects of a novel approach to the Diffie-Hellman (DH) problem. Many researchers favor the MQV protocol of Law, Menezes, Qu, Solinas and Vanstone because of its greater efficiency among the commonly known authenticated Diffie-Hellman protocols The MQV is specifically designed to achieve a remarkable list of security properties, including resistance to active man-in the-middle attacks. Recently, Hugo Krawczyk invented a Hashed MQV (HMQV) protocol, which involves the hashing of the party's own DH value and the peer's identity. HMQV is designed to overcome the security shortcomings of MQV, while preserving the efficient performance of MQV. Our protocol uses double hashing of the DH value and of the peer's identity. We expect to adapt our protocol to the Twin DH problem of Cash, Klitz and Shoup. Such studies have obvious applications in communication systems. (Received February 09, 2014)