1046-94-1517 **Yesem Kurt*** (ykurt@randolphcollege.edu), 2500 Rivermont Ave, Randolph College, Lynchburg, VA 24503. *An Identification Scheme for One-Time Private Key Systems (OTPK).* Preliminary report.

One-Time Private Key (OTPK) is a new technology for online digital signatures in Public Key Infrastructure (PKI) architecture. In PKI a user chooses a private key, computes the public key,and sends it to the Trusted Authority (TA) for certification. Once he/she receives his certificate, he/she can sign messages using the private key. The certificate is valid until it expires typically for months. The idea in OTPK is to use a new private key and a new certificate each time a document is signed. It has several advantages over regular PKI. In this talk we shall describe a signature scheme which assumes that the private key is used only once (hence could be used in an OTPK system). The scheme works over non-commutative structures and relies on triple decomposition problem in the structure. (Received September 16, 2008)