1056-94-1566 **Yesem Kurt-Peker*** (ykurt@randolphcollege.edu), Randolph College, 2500 Rivermont Ave., Lynchburg, VA 24503. *A Signature Scheme over Non-commutative Groups Secure Against Existential Forgery.* Preliminary report.

We shall introduce a new non-deterministic signature scheme which, under certain assumptions on the hash function used, is secure against existential forgery with adaptive chosen-message attacks when non-malleability is not part of the security requirements; that is producing a second signature to an already queried message does not count as forgery. Different from most signature schemes in use today, the new scheme is designed to work in non-commutative structures. The security of the scheme lies in the difficulty of the decomposition problem in the underlying group. For a concrete example we employ the group of matrices with entries from a finite field and discuss the complexity of operations involved. In the signing process, a user has to do some inversions and also choose elements from the centralizer of a given element. These are the costliest operations in the overall signature scheme. Verification requires 13 multiplications in the group, which, when considered over matrices is a fast operation. Solving the decomposition problem in the case of matrices amounts to solving multivariate polynomial equations which is known to be hard in general. (Received September 22, 2009)