1023-08-928 **Yesem Kurt*** (yesem.kurt@pomona.edu), Department of Mathematics, Pomona College, 610 N. College Ave, Claremont, CA. *A New Key Exchange Primitive.* Preliminary report.

A key exchange is a protocol by which two parties agree on a secret key to use in their subsequent private communication. We will present a new key exchange primitive whose security relies on what we call the triple decomposotion problem over non-commutative groups. The system is designed to overcome the vulnerabilities of previously proposed systems which also rely on some version of the decomposition problem. Different from the previous key exchange schemes where the problem is decomposing an element into three parts where the middle piece is known, our scheme relies on decomposing an element into three parts all unknown. This is the triple decomposition problem and it seems to be a harder problem because it requires quadratic systems to be solved instead of linear ones. We will discuss the new primitive over some non-commutative groups, particularly over matrices and give a setting for practical applications. (Received September 26, 2006)