TITLE: CRYPTOGRAPHIC COMMUNICATION PROCESS

ABSTRACT:

A novel asymmetrical cryptographic schema which can be used for enciphering, signature and authentication. The schema is based on low degree public polynomial equations with value in a finite ring K.

The mechanism is not necessarily bijective. The secret key makes it possible to hide polynomial equations with value in extensions of the ring K. The solving of these equations makes it possible, if one has the secret key, to execute operations which are not executable with the public key alone.

Fig. 1 to be published.