ABSTRACT

ASYMMETRIC CRYPTOGRAPHIC COMMUNICATION PROCESS
AND ASSOCIATED PORTABLE OBJECT

The invention relates to an asymmetric cryptographic communication process which establishes a correspondence between a first value (x) represented by n elements $(x_1,\ldots,x_n)$ of a ring (A) and a second value (y) represented by m elements $(y_1,\ldots,y_m)$ of this ring, n and m being integers greater than or equal to 2.

According to the invention:

- said correspondence is defined by multivariable public polynomials (P_i) of $A^{n+m+k} \rightarrow A$, with a low total degree, such that there are equations of the type $P_i(x_1,\ldots,x_n;\ y_1,\ldots,y_m;\ z_1,\ldots,z_k) = 0$, where $(z_1,\ldots,z_k)$ are possible intermediate variables and k is an integer;
- at least the majority of the polynomials (P_i) do not have the form $T_i(y_1,\ldots,y_m) = S_i(x_1,\ldots,x_n)$, where the S_is would be polynomials with a total degree of 2 and the T_is would be polynomials with a total degree of 1.

The invention also relates to an associated portable object.

Fig. 1 to be published.