(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 065 593 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
03.01.2001 Bulletin 2001/01

(51) Int Cl.[7]: **G06F 9/46**, G06F 1/00

(21) Application number: **99480057.1**

(22) Date of filing: **02.07.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **Institut Eurecom G.I.E.**
06904 Sophia-Antipolis (FR)

(72) Inventors:
- **Molva, Refik**
  06560 Valbonne (FR)
- **Loureiro, Sérgio**
  06250 Mougins (FR)

(74) Representative: **Schuffenecker, Thierry**
97, chemin de Cassiopée,
Domaine de l'étoile
06610 La Gaude (FR)

(54) Process for securing the execution of a mobile code in an untrusted environment

(57) A process is disclosed for securing the execution of a mobile code in a Information Handling System (I.H.S.) (30) having a function which can be represented on a matrix F . The function is being encrypted by means of an Error-Correcting Code (E.C.C.) transformation, where the code is preferably a GOPPA code. The transformation produces an encrypted matrix F' = FGP + E, where G is a generating matrix for an (n, k, d) algebraic block code C, P is a nxn random permutation matrix and E a kxn random matrix where at least n-t columns consists of a null vector. Since the Encrypted matrix F' is still a matrix, the mobile code which is encrypted is still executable in a user's environment.

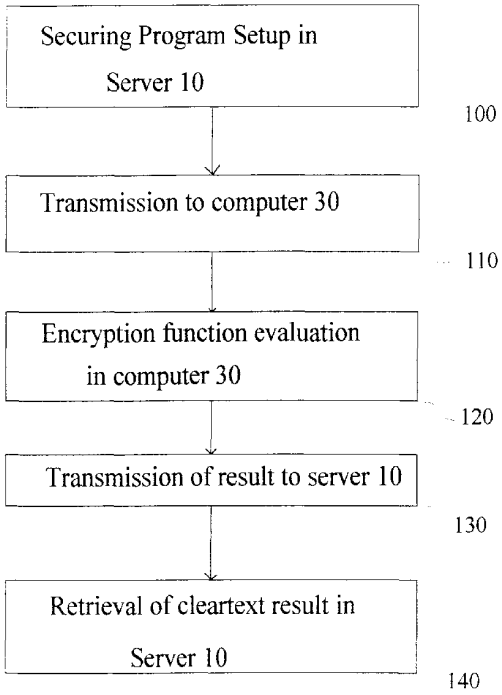

Fig. 2

EP 1 065 593 A1