

CRYPTOGRAPHY BY PARAMETERIZING ON ELLIPTIC CURVE

Abstract

5 The invention relates to the implementation of the control of a device (10) by a controller (11) on the basis of a password (π). For this purpose, the invention comprises determining (21), at the device or at the controller and on the basis of a random value r_1 , a point $P(X,Y)$ on an elliptic curve in a finite body F_q , q being an integer, according to the equation: $E_{a,b}(x,y) : x^3 + ax + b = y^2$ (1). The invention then

10 comprises obtaining (22) first and second parameters k and k' , such that $P(X,Y)=F(K,k')$, where F is a surjective function of $F_q \times F_q$, in F_q , and then obtaining (23) the first and second parameters in an encrypted format by encryption in accordance with the password. The invention finally comprises transmitting (24) the first and second encrypted parameters to the controller. During the control, the

15 function F is used, such that, whatever the values of z and z' , which are input elements of F_q , $F(z,z')$ is a point on the elliptic curve and the input elements do not satisfy the equation (1).

Fig. 2