

$$r_2.G = D_\pi E_\pi(r_2.G)$$

and the controller 11 recovers at a step 17 the random value r_1 generated by the device 10 by deciphering the information contained in the message 13:

$$r_1.G = D_\pi E_\pi(r_1.G)$$

5 Thus, following a protected exchange, each entity is able to calculate a common key K:

$$K = r_1.r_2.G$$

This type of algorithm aims to exchange values in a form encrypted with a password or a key derived from a password. However, it should be noted that
 10 according to a classical representation of an elliptic curve satisfying equation (1) on a finite field F_q , the exchanges described with reference to Figure 1 can allow a potential attacker to deduce information relating to the password π . In fact, exchanging random values in an encrypted form as described above, via the two messages 13 and 15, supplies a redundancy of information which may
 15 allow the secret of the password to be broken. More precisely, at each listening-in, an attacker could test a password to decipher the information exchanged in messages 13 and 15. He is then presented with two cases. In the first case, the decrypted information corresponds to a point on the curve and accordingly the password is correct. In the second case, the decrypted
 20 information does not correspond to a point on the elliptic curve and the password is not discovered. By multiplying the listenings-in and the separate passwords, it is thus possible to find the password belonging to a finite set of elements.

Embodiments of the present invention seek to improve the situation.

25 A first aspect of the present invention proposes a method of controlling a device by a controller on the basis of a password;
 said method comprising the following steps, at the device or at the controller:

/1/ on the basis of a random value r_1 , determine a point $P(X,Y)$ on an elliptic curve, in a finite field F_q , q being an integer, of equation:

30
$$E_{a,b}(x,y) : x^3 + ax + b = y^2 \quad (1)$$

/2/ obtain first and second parameters k and k' , such that

$$P=F(k,k')$$

-select at random an element u in the set $f_{a,b}^{-1}(P_t)$

- return u

It should be noted that, to obtain a $1-1/2^k$ probability of success, it is sufficient to have T equal to a polynomial evaluated in k of degree 1, in other words T is a multiple of k .

Moreover, the following steps can be employed:

- receive a message stating first and second parameters in a form encrypted with the password;
- decipher the first and second parameters and obtain parameters p and p' ; and
- calculate a common secret value K with the controller according to the following equation:

$$K = r_1 \cdot F(p, p')$$

where r_1 is the random value used at step /1/.

Thus, the device and the controller can finally have a common key at their disposal without exchanging information that puts the secrecy of the password in jeopardy.

In an embodiment, A second aspect of the present invention proposes an electronic entity comprising means suitable for implementing a method of control according to the first aspect of the present invention.

A second aspect of the present invention proposes an electronic entity in a system for control by password comprising:

- a determination unit suitable for determining a point $P(X,Y)$ on an elliptic curve in a finite field F_q , q being an integer, on the basis of a random value r_1 , the elliptic curve being of equation:

$$E_{a,b}(x, y) : x^3 + ax + b = y^2 \quad (1)$$

- an obtaining unit suitable for obtaining first and second parameters k and k' , such that

$$P = F(k, k')$$

where F is a surjective function of $F_q \times F_q$ in F_q .

- an encryption unit suitable for obtaining the first and second parameters in encrypted form by encryption as a function of the password; and

- an interface unit suitable for transmitting said first and second encrypted parameters to the controller;

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

5 A third aspect of the present invention proposes a system of control by password comprising at least a first electronic entity according to the second aspect as controller and a second electronic entity according to the second aspect as device to be controlled.

10 Other aspects, aims and advantages of the invention will become clear on reading the description of one of its embodiments.

The invention will also be better understood with the aid of the following figures:

- Figure 1, already described, illustrates the main steps of a method of control according to the prior art;
- 15 - Figure 2 shows the main steps of a method of control according to one embodiment of the present invention;