

AUTHENTICATION DEVICE, AUTHENTICATION METHOD, AND PROGRAM

ABSTRACT

5

Provided is an authentication device including a key holding unit for holding L ($L \geq 2$) secret keys s_i ($i = 1$ to L) and L public keys y_i that satisfy $y_i = F(s_i)$ with respect to a set F of multivariate polynomials of n -th order ($n \geq 2$), and an interactive protocol execution unit for performing, with a verifier, an interactive protocol for proving knowledge of $(L-1)$ secret keys s_i that satisfy $y_i = F(s_i)$. The interactive protocol execution unit includes a challenge reception unit for receiving L challenges Ch_i from the verifier, a challenge selection unit for arbitrarily selecting $(L-1)$ challenges Ch_i from the L challenges Ch_i received by the challenge reception unit, a response generation unit for generating, by using the secret keys s_i , $(L-1)$ responses Rsp_i respectively for the $(L-1)$ challenges Ch_i selected by the challenge selection unit, and a response transmission unit for transmitting the $(L-1)$ responses Rsp_i generated by the response generation unit to the verifier.

10

15

Fig. 9