Abstract

Method and Apparatus for Swarm Authentication of a Plurality of Proving Devices by Using Distributed Identification Schemes

A method and apparatus are disclosed and claimed which enable a plurality of proving devices to collectively generate proofs of network identity of messages that everyone (hereafter the verifying device) can verify but no one can forge. Compared to other schemes of this type (such as RSA signatures), the inventive identification schemes are faster by at least one or two orders of magnitude. In the present invention disclosed and claimed in this patent application, a number of improved variants of the Fiat-Shamir scheme are described which allow the verifying device to interact, in a single protocol, with a plurality of connected objects. The proposed protocol is energy efficient: unless the network topology does not allow vicinity routing, each connected object will communicate only with one connected object at its vicinity. Connected objects progressively consolidate messages and forward those messages to each other until one consolidated message eventually reaches the verifying device. Moreover, in this invention disclosed and claimed in this patent application, a number of improved variants of Schnorr identification scheme are also described which allow the verifying device to interact, in a single protocol, with a plurality of connected objects.

Fig. 1