SYSTEM AND METHOD FOR COMPUTING PRIVATE KEYS FOR SELF CERTIFIED IDENTITY BASED SIGNATURE SCHEMES

Abstract

This document describes a system and method for generating private keys for devices participating in a self-certified identity based encryption scheme whereby the private key is used by the devices to establish a common session key for encoding digital communications between devices.

FIGURE 3