ABSTRACT

At the moment of the diffusion of Pay-TV with multi-channel signals, each channel is associated to authorization messages (ECM) which allow to decrypt this channel according to the rights of the subscriber. When changing channel, a very short time is accepted before one has determined these new rights in relation with the new channel. The heavy encrypting algorithms are thus excluded. To avoid this drawback, to decrypt a channel, a system is proposed using the combination of the authorization information for a channel (ECM), and thus encrypted by a fast algorithm, with authorization information (MECM) for a group of channels. These latter are encrypted by a high security algorithm and are thus slower to decrypt.



162162



G00002