

H 04 N

Ans.nr.: 2554/84

Indleveret: 24 maj 1984

Løbedag: 24 maj 1984

Alm. tilgængelig: 28 nov 1984

Prioritet: 27 maj 1983 US 498800

*M/A-COM LINKABIT INC.; San Diego, US.

Opfinder: Klein S. *Gilhouser; US, Charles F.

*Newby Jr.; US.

Fuldmægtig: Firmaet Chas. Hude

Nøglesignalkryptografering

SAMMENDRAG

2554-84

Fremgangsmåde og apparat til kodning og selektiv dekodning af fjernsynssignaler, der transmitteres til abonnenters dekodere i et abonnent-TV-system. Et arbejdsnøglesignal genereres ved en signalbehandling af et begyndelsesvektorsignal i overensstemmelse med en DES-algoritme, ved at algoritmen nøgles ved hjælp af et fælles kategorinøglesignal eller ved hjælp af et signal med en forudbestemt relation til det fælles kategorinøglesignal. En unik kryptograferingsnøglestøm genereres ved en signalbehandling af begyndelsesvektorsignalet i overensstemmelse med DES-algoritmen, ved at algoritmen nøgles ved hjælp af arbejdsnøglesignalet. Et fjernsynssignal kodes i overensstemmelse med den unikke kryptografinøglestøm til tilvejebringelse af et kodet fjernsynssignal. Et antal unikke kryptograferede kategorinøglesignaler, der er individuelt adresseret til forskellige abonnenters dekodere er genereret ved en behandling af begyndelsesværdien af det fælles kategorinøglesignal i overensstemmelse med DES-algoritmen, ved at algoritmen nøgles ved hjælp af forskellige "enhedsnøgle-

signaler", der er unikke i forhold til forskellige udvalgte dekodere. Det kodede fjernsynssignal, begyndelsesvektorsignalet og antallet af kryptograferede kategorinøglesignaler udsendes til dekomoderne. En tilsvarende række af DES-algoritmer anvendes ved dekomoderen til at reproducere kryptografinøglestømmen, og TV-signalet dekoderes i overensstemmelse dermed. Den enkelte dekomoderes unikke enhedsnøglesignal lagres i en sikker hukommelse til brug ved reproduktion af det fælles kategorinøglesignal, når dekomoderen adresseres ved hjælp af sit unikke kryptograferede kategorinøglesignal.

2554-84

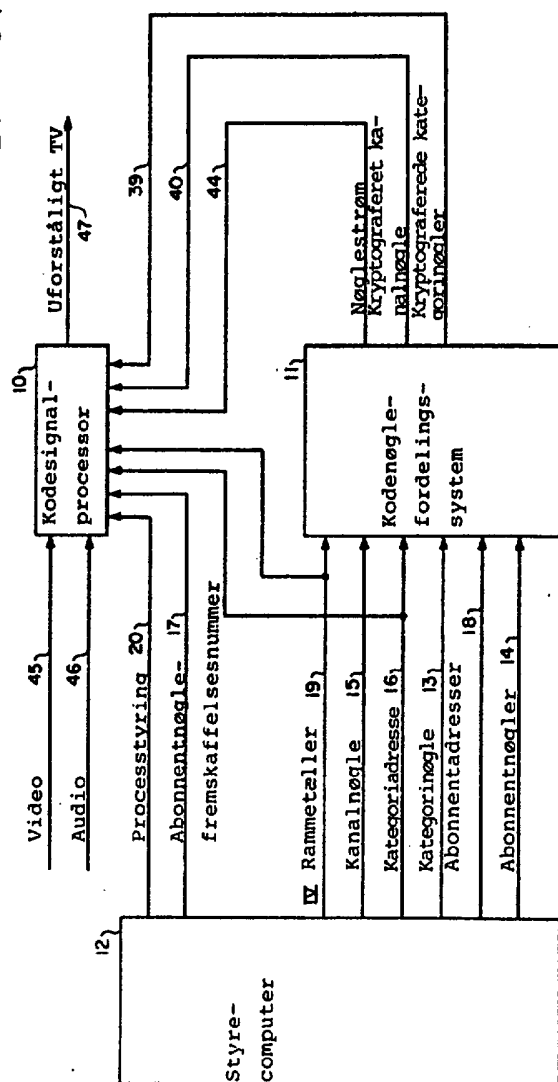


FIG. 1