



SUOMI-FINLAND
(FI)

Patentti- ja rekisterihallitus
Patent- och registerstyrelsen

[A] TIIVISTELMÄ - SAMMANDRAG

(11) (21) Patenttihakemus - Patentansökan 923481

(51) Kv.1k.5 - Int.cl.5

H 04L 1/08, H 04L 9/00

(22) Hakemispäivä - Ansökningsdag 31.07.92

(24) Alkupäivä - Löpdag 31.07.92

(41) Tullut julkiseksi - Blivit offentlig 02.02.93

(32) (33) (31) Etuoikeus - Prioritet

01.08.91 DE 4125812 P

(71) Hakija - Sökande

1. Siemens Aktiengesellschaft, Wittelsbacherplatz 2, 8000 München, BRD, (DE)

(72) Keksijä - Uppfinnare

1. Gückel, Hartmut, Burgkamp 4 A, 3150 Peine, BRD, (DE)

(74) Asiamies - Ombud: Oy Kolster Ab

(54) Keksinnön nimitys - Uppfinningens benämning

Menetelmä signaaliteknisesti varmaa tiedonsiirtoa varten
Förfarande för signaltekniskt säker dataöverföring

(57) Tiivistelmä - Sammandrag

Keksintö koskee menetelmää signaaliteknisesti varmaa tiedonsiirtoa varten. Siirto-menetelmä koskee vähintään kaksinkertaista tiedonsiirtoa, jolloin siirrettävä tietosanomapari (T1.1, T2) esitetään sopivien toimenpiteiden avulla tilastollisesti toisistaan riippumattomina bittijonoina. Tämä saavutetaan käyttämällä salausteknistä koodausmenetelmää ainakin toiseen lähdessä generoituun tietojonoon. Näin tehtäessä todennäköisyys, että kulloinkin yhteenkuuluvat tietosanomat vääristyisivät häiriövaikutuksien johdosta siten, että niiden vääristymä ei enää olisi kohdepäässä tietojen vertailun avulla havaittavissa, on merkityksettömän pieni. Keksinnön mukainen menetelmä aikaansaa signaalitek-nisesti varmasti toteutetun lähteen (Q) ja kohteen (S) yhteydessä signaalitek-nisesti varman tiedonsiirron signaalitek-nisesti epävarman tiedonsiirtojärjestelmän kautta, jonka toteutus voi olla täysin tuntematon.

Uppfinningen avser ett förfarande för signaltekniskt säker dataöverföring. Överföringsförfarandet omfattar åtminstone en dubbel dataöverföring, varvid datatelegramparen (T1.1, T2), som skall överföras medelst lämpliga åtgärder framställs som statistiskt av varandra oberoende bitföljder. Detta ernås med användning av ett kryptotekniskt kodningsförfarande på åtminstone den ena på källsidan genererade dataföljden. På detta sätt blir sannolikheten för att respektive samhöriga datatelegram genom störningsinverkan skulle förvrängas så, att förvrängningen ej mera kunde konstateras genom datajämförelse på målsidan, försumbart liten. Det uppfinningsenliga förfarandet tillåter i förening med signaltekniskt säkert utformad källa (Q) och mål (S) den signaltekniskt säkra dataöverföringen gentemot ett signaltekniskt osäkert dataöverföringssystem, vars utföringssätt kan vara fullkomligt obekant.

